ExtremeWare Release Notes

Software Version 7.2.0b37

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: November 2004
Part Number: 120182-00 Rev 10

Alpine, Altitude, BlackDiamond, EPICenter, Ethernet Everywhere, Extreme Ethernet Everywhere, Extreme Networks, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, GlobalPx Content Director, the Go Purple Extreme Solution Partners Logo, ServiceWatch, Summit, the Summit7i Logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and other countries. Other names and marks may be the property of their respective owners.

© 2004 Extreme Networks, Inc. All Rights Reserved.

Specifications are subject to change without notice.

NetWare and Novell are registered trademarks of Novell, Inc. Merit is a registered trademark of Merit Network, Inc. Solaris is a trademark of Sun Microsystems, Inc. F5, BIG/ip, and 3DNS are registered trademarks of F5 Networks, Inc. see/IT is a trademark of F5 Networks, Inc.

All other registered trademarks, trademarks and service marks are property of their respective owners.

Author: Susan Lynott

Editor: Rich Small

Production: Susan Lynott

Special Thanks: Paul, Sridhar

Contents

Chapter 1 Overview

New Features in ExtremeWare 7.2.0b25 **11**

Features Added or Enhanced in ExtremeWare 7.2.0b25 11

System Health Check Scan Recovery *11*

Packet Memory Scan Behavior Modification *12*

Clear Packet Memory Diagnostics Failures *12*

Clear Alpine Diagnostics Failures *12*

Capture Corrupted Packet Data *13*

Serial Numbers now Included in Command Output and Log Messages *13*

Backplane Failure Error Messages *13*

New Diagnostics Output Options *13*

Alpine Power Checking for PoE Modules *13*

New backplane mapping Option *14*

Features Added or Enhanced in ExtremeWare 7.2.0b18 14

Power over Ethernet *14*

XENPAK Support *14*

DHCP Option 82 *14*

QoS Monitor *14*

Application Examination *14*

New MIB and Traps *15*

P-MIB and Q-MIB *15*

Selective Forwarding for ESRP-Aware Switches *15*

Supported Hardware **15**

BlackDiamond Component Support 16

Alpine Component Support 17

Summit Component Support 18

GBIC Support 18

Mini-GBIC Support *19*

XENPAK Module Support 19

Chapter 2 Upgrading to ExtremeWare 7.2

Staying Current 21

Upgrading ExtremeWare 21

Upgrading Switches to ExtremeWare 7.2.0 22

Save the Current Configuration 22

Upgrade the BootROM to Version 8.1 23

Upgrade to ExtremeWare 6.1.9 23

Upgrade to ExtremeWare 6.2.2b56 23

Upgrade to ExtremeWare 7.2.0b37 24

Upgrade T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79 25

Upgrade T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later 26

Upgrade ATM, MPLS, ARM, or PoS Modules from a Release Prior to ExtremeWare 6.1.8b79 26

Upgrading an Alpine 3802 to ExtremeWare 7.2.0b37 27

Downgrading Switches 27

Chapter 3 Supported Limits

Supported Limits 29

Chapter 4 Clarifications, Known Behaviors, and Resolved Issues

Clarifications and Known Behaviors 35

General 35

Changing Port Speed Stops Packet Transmission 35

Creating an ACL with a Filter-Precedence Generates a Conflict Error 35

Error Message While Hot-Removing Line Cards 36

System Related – All Systems 36

Autonegotiation Setting Not Preserved on Added and Deleted Loopback Ports 36

The show log Command Truncates Long Commands 36

The show log Display Truncates Configuration Parsing 36

Do Not Create Single-Character Names 36

Telnet and the show ports Command 36

The show configuration Output 36

LACP not Supported 36

Upgrading to ExtremeWare 7.0 and Bi-Directional Rate Shaping 37

Upgrading to ExtremeWare 7.0 and OSPF 37

Blank Space in show port info detail Command Output 37

Using an ExtremeWare 7.0 Configuration with an Earlier Image 37

Console Response with a Large Number of ARP Entries 37

The show log chronological Command 37

BOOTP-Dependent Routes in Downloaded Configuration not Created 37

BlackDiamond 37

Changing Address-Based Algorithms to L2_L3 Does Not Preserve After Save and Reboot 37

Cross-Module Trunking and Hitless Failover 38

Autonegotiation Off Command Accepted on 10 Gigabit Ethernet Modules 38

Disabling One MSM Might Cause Loss of Throughput 38

Cannot Delete an LSP Previously Referenced by a TLS Tunnel 38

10 Gigabit Ethernet and CMT 38

XENPAK with the BlackDiamond 6816 38
Cross-Module Trunking Not Supported on MSM64i's 38
Cross-Module Trunking Module Support 38
Master Slot Must Be Active for CMT 39
MSM-3 Log Might Be Out of Chronological Order 39
Source Addresses Might Age Out of FDB 39
Do Not Use Static FDB Entries with CMT 39
Saving Health Check Configuration After Failure Causes Console Crash 40
Diagnostics on MSM-3 with Hitless Failover Causes Failover and Spurious Message 40
Do Not Configure a Port-Based Backplane Algorithm When CMT is Enabled 40
Cross-Module Trunking and ACLs 40
4,000 VLANs on a BlackDiamond 40
PPP Links Through E1 modules 40
Slot Failure Messages During a Broadcast Storm 40
No Image Information Reported to SNMP with One MSM 40
BlackDiamond 6816 MSM C and D Diagnostics Messages not in Syslog 40
Disabling CLI Paging from the Slave MSM64i 41
The unconfig switch all Command 41
BlackDiamond 6816 MIB Value for Input Power Voltage 41
Alpine 41
Mirroring Failure on an Alpine3808 with GM4x Card After a Save and Reboot 41
Logs with attachment.Autonegotiation on VDSL Ports Set Incorrect Speed 41
VDSL Ports do not Support Jumbo Frames 41
Status LED Solid After Fan Tray Reseated 41
New Accounts with WAN Module Installed are pppuser 41
Traffic Diagnostics Not Performed During Extended Diagnostics on T1 Module 42
Traffic Diagnostics Not Performed During Extended Diagnostics on E1 Module 42
Limited Commands Mode 42
VDSL Modules in a Half-Duplex Link 42
Summit 42
Summit48i Fiber Link Does Not Recover After Link Goes Down 42
Spurious Summit48si Power Supply Messages 42
Using Vista to Add and Delete Ports 42
Output of the show log Command 42
The unconfigure switch all Command Clears the Default VLAN from s0 43
Health Check Error Messages 43
SNMP Results for Power Sources 43
Command Line Interface (CLI) 43
Console Does not Wait for User Input 43
The show ports mgmt info Output Missing Flags 43
Press [Return] Key Twice With enable temperature-log Command 43
User Sessions Cannot Enable CLI Paging 43
Switching and VLANs 44
The show iproute Output 44
MAC-Based VLAN Configuration Not Saved 44
Load Share Group Might Fail Back to Group with Fewer Ports When Using Software Redundant Ports 44
Saving ip-mtu Settings 44
VLAN priority and STP, EDP 44
Default Routes or Static Routes 44

Configuring a Protocol Filter with 'ffff' 44
Deleting Protocols from a VLAN 45
MAC Based VLANs and DHCP Relay 45
VLAN to VLAN Access Profiles 45
FDB 45
Cannot Add FDB Entry for Management VLAN 45
Static FDB Entries and Rate-Shaping 45
MAC Security 45
Load Sharing 45
Autonegotiation 45
Round Robin Load Sharing 45
Port Based Load Sharing on Summit7i 45
Alpine and Cross Module Load Sharing 46
Load Sharing and Specific Ports in a Load Share Group 46
Disabling Load Sharing if the Master is Down Generates Error 46
ELSM 46
Spurious Error Message with ELSM 46
Spanning Tree 46
Disabling ignore-bpdu Adds CPU MAC Entry to FDB 46
Enabling STP on MAC-based VLANs Might Cause Connectivity Loss 46
Incorrect Log Message 46
Disabling STP Might Display Topology Change 46
FDB Not Flushed After Link Failure with RSTP 47
Error Messages with Topology Changes 47
Large STPD Configuration Download Might Reboot Switch 47
A Large STP Configuration with 10 Link Transitions 47
Configure Fewer than 4,000 VLANs in an STPD 47
Output of show stpName port detail Command in Hex Format 47
If You Delete a Port from the STPD, You Cannot Add It Through a VLAN 47
The unconfigure stp Command Does Not Clear All Configurations 47
Enabling ignore-bpdu or ignore-stp 47
Configuring a VLAN from Vista 48
STP and VLAN Tagging 48
EMISTP and Ingress Rate Shaping 48
ESRP 48
The disable slot all Command Generates EDP Errors 48
Large Configurations Might Lock Console when Enabling and Disabling s0 48
Hot-Swapping a Module with 5,000 ACLs 48
ELRP 48
ELRP and Ingress Rate Shaping 48
VRRP 49
Backup Transition Creates Duplicate Packets 49
QoS 49
Duplicate Precedence Rules 49
The qosprofile Accepts a Value Greater than 100% 49
Access Lists Using the IP Deny Any Rule 49
Access Lists and IP Fragmentation 49
QoS Configuration Bandwidth Parameters 49
Creating Access Lists from Multiple Sessions 49

Bi-Directional Rate Shaping 50
Locking and Unlocking Learning 50
Loopback Port Must be on Same Module 50
1000Base-T Ports as Loopback Ports 50
EAPS 50
Do Not Configure a Hello Time of 0 50
EAPS Performance Statistics 50
ESRP and EAPS Secondary Port 51
Incorrect show vlan Output 51
IP Unicast Routing 51
Reset the FDB Aging Timer 51
Multinetting and the show VLAN stats Command 51
Multinetting and VRRP 51
RIP Routing 51
RIPv2 Authentication 51
RIP in Conjunction with other Routing Protocols 51
OSPF 52
OSPF Originate Default Cost Can Be Set Incorrectly 52
LSA Batch Interval Not Supported 52
Static Route with Switch's Address as Gateway Not Advertised 52
Error Message Not Generated 52
Disable OSPF Before Adding or Removing External Area Filters 52
IS-IS 52
Unicast Packets Considered Broadcast 52
BGP 52
Large Number of Access Profiles and a Peer Reset 52
Default Route Might Not Be Deleted 52
BGP Aggregation with a Maximum Prefix of 300,000 53
IP Multicast Routing 53
The unconfigure igmp Command Does Not Unconfigure All Parameters 53
Enable or Disable IGMP Snooping on a Sub-VLAN 53
Do Not Disable IGMP Snooping with Static Snooping Entries 53
Cisco Interoperation 53
Traffic Rate Exceeding Last Hop Threshold 53
Security and Access Policies 53
Roaming Client MAC Might be Aged Out 53
The show netlogin Output Might Display Wrong Authentication 53
ICMP Access Lists and ignore-overlap 54
CPU DoS Protect and ACL Precedence 54
Network Login RADIUS Server Interoperability 54
Network Login Supplicant Software Interoperability 54
RADIUS and the BlackDiamond 54
SLB and Flow Redirection 55
Enumeration Mode Redirects ICMP Packets 55
Cache Servers Set To "Down" Under Sustained High Traffic Loads 55
Health Checking Cannot be Disabled 55
NAT 55
NAT Rule Configuration Not Updated 55

Vista 55
Failed Vista Login Logged Incorrectly *55*
Failed Vista Login Logged Incorrectly *55*
No 10 Gigabit Option for Port Speed *55*
Incorrect Minimum Limit on OSPF Page *56*
Cannot Create User Accounts *56*
Cannot Enable STP *56*
Alpine 3808 Erroneously Displays Four PSUs *56*
Cannot Add Trap Receiver or Community String *56*
Blackhole Flag Missing *56*
Multicast Address Display *56*
Configuration Statistics PSU Display *56*
Vista and RADIUS *56*
Configuration Options with Large Number of Interfaces *56*
SNMP 57
The configure snmp community Command Replaced *57*
Only Warm Start Smart Trap Sent After Power Cycle *57*
Cannot Delete Default Community Strings *57*
Do Not Configure an SNMPv3 Community String with more than 32 Characters *57*
Modular Switch get Error *57*
Incrementing the Interface Value *57*
SNMP Access Profile *57*
SNMP and Auto-negotiation Settings *57*
Extreme Fan Traps *58*
Extreme Power Supply Traps *58*
Diagnostics and Troubleshooting 58
Errors Not Displayed in show diagnostics Output *58*
Entering q Does Not Quit Diagnostics Display *58*
Automatic Memory Scanning Can Trigger Incorrect Reboot Loop Detection *58*
Packet Diagnostics Display Backplane Incorrectly *58*
Packet Diagnostics Display Wrong Slot Name *58*
Bus-Stats Error Messages *58*
Spurious Message When system-down is Configured *59*
The use configuration Command *59*
Output of the show diagnostics Command *59*
Configure Auto-Recovery to online or Alarm-Level to traps *59*
Configuring Diagnostics Mode Off *59*
Disable Remote Syslog Before Enabling IPARP Debug-Tracing *59*
Documentation 59
The Auto-Recovery Threshold Applies only to BlackDiamond I/O Modules *59*

Issues Resolved in ExtremeWare 7.2.0b37 **60**
Diagnostics 60
EAPS 60
EDP 60
General 60
PIM 60
SLB 60
SNMP 60

SSH 61
STP 61
VRRP 61

Issues Resolved in ExtremeWare 7.2.0b33 61
General 61
CLI 62
BlackDiamond 62
Summit 63
Mirroring 63
Multicast 63
Bridging 63
BGP 63
EAPS 63
IP Routing 63
OSPF 63
System Related – All Systems 63
Security and Access Policies 64
STP 64
SNMP 65
Switching and VLANs 65
MPLS 65
VRRP 65
ESRP 65
Documentation 65

Issues Resolved in ExtremeWare 7.2.0b25 66
General 66
BlackDiamond 66
Alpine 66
Summit 66
Mirroring 66
STP 66
ESRP 67
EAPS 67
OSPF 67
IP Multicast 67
PIM 67
SLB and Flow Redirection 67
Security 67
SNMP 68
Troubleshooting 68

Issues Resolved in ExtremeWare 7.2.0b18 **68**
General 68
ESRP 68
OSPF 68
SNMP 69
Vista 69
Troubleshooting and Diagnostics 69

1 Overview

These Release Notes document ExtremeWare® 7.2.0b37. ExtremeWare 7.2.0 enables new hardware products and software features.

NOTE

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2 (or later). To install ExtremeWare 7.2, see "Upgrading ExtremeWare" on page 21.

This chapter contains the following sections:

- New Features in ExtremeWare 7.2.0b25 on page 11
- Supported Hardware on page 15

New Features in ExtremeWare 7.2.0b25

Following are descriptions of features introduced or enhanced in ExtremeWare 7.2.0b25. These features are documented in detail in the *ExtremeWare Software User Guide* or the *ExtremeWare Software Command Reference Guide*, unless otherwise noted.

You can ignore numbers in parentheses, which are for internal use.

Features Added or Enhanced in ExtremeWare 7.2.0b25

The following features were added or enhanced in ExtremeWare7.2.0b25.

System Health Check Scan Recovery

Extreme Networks support personnel can now configure the action taken by the system health check if diagnostics are run or if checksum errors trigger diagnostics. If diagnostics are run or triggered in previous releases of ExtremeWare, the module is reset and diagnostics are run. Support personnel can use the following command to configure ExtremeWare to simply to reset the module without running diagnostics:

```
configure sys-health-check scan-recovery [reset | remap]
```

Entering this command generates the following message:

```
This command should only be used at the direction of Extreme Personnel. Do you wish
you continue (y/n)?
```

Answering `y` immediately implements the change. Answering `n` implements no change and returns you to the command line.

Use the `reset` option to reset the module without running diagnostics. This option is useful for recovering from transient hardware failures. In these cases, resetting the module stops the checksum errors.

Use the `remap` option to reset the module and run diagnostics. This is the default.

This command is not available on the BlackDiamond 6816.

This command is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Packet Memory Scan Behavior Modification

If you configure the system health check mode to `offline` and no new errors are detected, the device scanned now remains online. This behavior is identical to the current behavior if you use the `run diagnostics` command.

This behavior is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Clear Packet Memory Diagnostics Failures

Extreme Networks support personnel can now clear the packet memory diagnostics failures from the EEPROM using the following command:

```
clear log diag remap <slot>
```

This command clears any error remapping. Use this command only at the direction of Extreme Networks personnel.

This command is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Clear Alpine Diagnostics Failures

Extreme Networks support personnel can now clear the Alpine diagnostics failures from the NVRAM using the following command:

```
clear log diag error <slot>
```

Use this command only at the direction of Extreme Networks personnel.

This command is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Capture Corrupted Packet Data

Extreme Networks support personnel can now capture corrupted packet data to help in troubleshooting problems using the following command:

```
show packet miscompare <slot> {verbose}
```

Use this command only at the direction of Extreme Networks personnel.

This command is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Serial Numbers now Included in Command Output and Log Messages

Serial numbers are now included in the output of the `show diagnostics` command. Component intitialization messages now include the component serial number. In addition, checksum errors now include the serial number of the module.

The output and messages are not documented in the *ExtremeWare 7.2 Software User Guide*, the *ExtremeWare 7.2 Command Reference Guide*, or the *Error Message Decoder*.

Backplane Failure Error Messages

If a BlackDiamond backplane connection fails, error messages similar to the following are generated:

```
<Crit:SYST> MSM-A HW_AN=0 SW_AN=0 DECODE=0 INTSTAT=0 ANRCVCFG=0 CTRL=10000000
<Crit:SYST> slot 2 HW_AN=ab SW_AN=10 DECODE=1 INTSTAT=bf8 ANRCVCFG=41a0 CTRL=ff3ffc00
<Crit:SYST> MSM-A=[701021-00-17 0235F-70766]
<Crit:SYST> slot 2=[701026-00-05 0019F-14981]
<Crit:SYST> backplane=701058-00-01 0235H-00105
```

In addition, if the connection between the backplane and a specific ports fails, the port number is now included in the error message.

These messages are not documented in the *ExtremeWare 7.2 Software User Guide*, the *ExtremeWare 7.2 Command Reference Guide*, or the *Error Message Decoder*.

New Diagnostics Output Options

The configure diagnostics command now has two new options, indicated in bold:

```
configure diagnostics [extended | fastpost | normal | off | verbose | quiet]
```

If you select `verbose`, the results of every test are recorded in the log. The `verbose` option is not saved through a reboot. Diagnostics end with a system reboot, so you must reconfigure verbose mode after running diagnostics.

If you select quiet, only the pass or fail result is recorded in the log. The default is `quiet`.

These options are not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Alpine Power Checking for PoE Modules

PoE modules require more power than other I/O modules. When a chassis containing a PoE module is booted or a new PoE module is inserted, the power drain is calculated. If the chassis is booting up, I/O modules are powered up, beginning with slot 1, until the PoE module. Before the PoE module is

powered up, the chassis calculates the power budget and powers up the PoE module only if there is enough power. The chassis then powers up as many additional I/O modules as possible.

If a PoE module is inserted into a chassis, the chassis calculates the power budget and only powers up the PoE module if there is enough power. Installed modules are not affected. However, if you reboot the chassis, power checking proceeds as described in the previous paragraph.

If you remove a PoE module, power is redistributed. If there is now enough power, I/O modules that were not powered up previously are powered up.

Before you install your PoE module, consult your sales team to determine the required power budget.

This feature is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

New backplane mapping Option

The `show diagnostics` command now has the `backplane mapping` option. This option displays the traffic mapping to all backplane links on the BlackDiamond system (PD2-199995201).

This option is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Features Added or Enhanced in ExtremeWare 7.2.0b18

The following features were added or enhanced in ExtremeWare 7.2.0b18.

Power over Ethernet

You can now provide power over Ethernet using the FM-32Pi module in an Alpine chassis.

XENPAK Support

The XENPAK 10 Gigabit Ethernet optical transceiver is now supported.

DHCP Option 82

In accordance with RFC 3046, you can now allow a client's PC to have automatic IP configuration via DHCP enabled while still always getting the same IP address.

QoS Monitor

The QoS monitor is a utility that monitors the eight hardware queues (QP1-QP8) associated with any port(s). The QoS monitor keeps track of the number of frames and the frames per second that a specific queue is responsible for transmitting on a physical port. Two options are available: a real-time display, and a separate option for retrieving information in the background and writing it to the log.

Application Examination

You can now configure ingress queue classification based on application QoS. This is especially useful for applications such as VoIP.

New MIB and Traps

SNMP MIB support for High Density Ethernet I/O modules including ingress QoS, and Exceed-Committed-Rate SNMP Trap and Syslog support for ingress QoS on High Density Ethernet I/O modules.

P-MIB and Q-MIB

The standard RFC 2674.1P and RFC 2674.1Q VLAN MIBs are now supported.

Selective Forwarding for ESRP-Aware Switches

You can now configure ESRP-aware VLANs to forward ESRP PDUs only on relevant ports. This avoids unnecessary traffic. To do this, create a port list by adding or deleting ports for the ESRP groups associated with an ESRP VLAN. The port list is maintained only for forwarding the ESRP PDUs. These ports must both be in the same ESRP group and be connected to switches running ESRP on the same link. Each ESRP group in the VLAN has a different port list.

When the ESRP-aware switch receives the ESRP PDU, the PDU is processed and forwarded to the ports listed in the portlist for that group (PD2-118770301).

To add ports for selective forwarding, use the following command:

```
configure vlan <vlanname> esrp group <group#> add esrp-aware-ports <portlist>
```

To delete ports from the selective forwarding list, use the following command:

```
configure vlan <vlanname> esrp group <group#> delete esrp-aware-ports <portlist>
```

To view the ports on the port list, use the following command:

```
show esrp-aware-ports [vlanname]
```

This feature is not documented in the *ExtremeWare 7.2 Software User Guide* or the *ExtremeWare 7.2 Command Reference Guide*.

Supported Hardware

Hardware in the following sections listed in *italics* is new for this release.

ExtremeWare 7.2.0b37 (and later) supports "*i*" series or "3" series products *only*.

Table 1 lists software filenames for the hardware that requires software.

Table 1: Software for supported hardware

Extreme Hardware	ExtremeWare Filename	BootROM Filename/Version
BlackDiamond 6816	v720b37.Gxtr or v720b37.SGxtr	Ngboot8.1.bin/8.1
BlackDiamond 6808	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
BlackDiamond 6804	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
Alpine 3808	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
Alpine 3804	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1

Table 1: Software for supported hardware (continued)

Extreme Hardware	ExtremeWare Filename	BootROM Filename/Version
Alpine 3802	v720b37.xtr or v720b37.Sxtr/EW-70-3802.mig	Ngboot8.1.bin/8.1
Summit7i/7iT	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
Summit1i/1iT	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
Summit5i/5iT/5iLX	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
Summit48i	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
Summit48si	v720b37.xtr or v720b37.Sxtr	Ngboot8.1.bin/8.1
ARM module	v720b37.arm	v720b37.nprom/1.18
OC3 PoS module	v720b37.oc3	v720b37.nprom/1.18
OC12 PoS module	v720b37.oc12	v720b37.nprom/1.18
OC3 ATM module	v720b37.atm3	v720b37.nprom/1.18
MPLS module	v720b37.mpls	v720b37.nprom/1.18
T1 module	v720b37.t1	t1boot28.wr/2.8
E1 module	v720b37.e1	e1boot28.wr/2.8
T3 module	v720b37.t3	t3boot28.wr/2.8

NOTE

The BlackDiamond 6816 requires its own ExtremeWare image. The image that runs on other BlackDiamond, Alpine, or stackable switches does not support the BlackDiamond 6816.

BlackDiamond Component Support

BlackDiamond components supported with ExtremeWare 7.2.0b37, and the minimum ExtremeWare version required by the chassis to support each component, include:

Table 2: BlackDiamond component support

BlackDiamond Component	ExtremeWare Required
BlackDiamond 6804	6.2.2b56[1]
BlackDiamond 6808	6.2.2b56[1]
BlackDiamond 6816	6.2.2b56[1]
MSM-3	7.1.1
MSM64i	6.2.2b56[1]
G8Xi	6.1.3
G8Ti	6.1.3
G12SXi	6.1.4
G16X[3]	7.0.1
G24T[3]	7.0.1
F32Fi	6.1.8
F48Ti	6.1.2
F96Ti	6.1.8
WDMi	6.1.5

Table 2: BlackDiamond component support (continued)

BlackDiamond Component	ExtremeWare Required
10GLRi	7.0
10GX3	7.2.0b18
MPLS	7.0
ARM	7.0
P3cMi	7.0
P3cSi	7.0
P12cMi	7.0
P12cSi	7.0
A3cMi	7.0
A3cSi	7.0
DC Power Supply	6.1.5
110 VAC Power Supply	6.1.5
220 VAC Power Supply	6.1.5

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

NOTE

Do not install mixed versions of the power supplies in the same system. Install power supplies of the same type.

Alpine Component Support

Alpine components supported with ExtremeWare 7.2.0b37, and the minimum ExtremeWare version required, include:

Table 3: Alpine component support

Alpine Component	ExtremeWare Required
Alpine 3802	6.2.2b56[1]
Alpine 3804	6.2.2b56[1]
Alpine 3808	6.2.2b56[1]
SMMi	6.2.2b56[1]
GM-4Si/Xi/Ti	6.1.5
GM-16X[3]	7.0.1
GM-16T[3]	7.0.1
FM-32Ti	6.1.5
FM-24MFi	6.1.5
FM-24Ti	6.1.7
FM-24SFi	6.1.7
FM-32Pi	7.2.0b18

Table 3: Alpine component support (continued)

Alpine Component	ExtremeWare Required
GM-WDMi	6.1.8
WM-4T1i	7.0.1
WM-4E1i	7.0.1
WM-1T3i	7.0.1
FM-8Vi	7.0.1
AC Power Supply	6.1
DC Power Supply	6.1.5

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

Summit Component Support

Summit components supported with ExtremeWare 7.2.0b37, and the minimum ExtremeWare version required, include:

Table 4: Summit component support

Summit Component	ExtremeWare Required
Summit1i	6.2.2b56[1]
Summit5i	6.2.2b56[1]
Summit7i	6.2.2b56[1]
Summit7i DC Power Supply	6.2.2b56[1]
Summit48i	6.2.2b56[1]
Summit48si	6.2.2b56[1]
Summit48si DC Power Supply	7.1.1[2]

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.
2. ExtremeWare 6.2.2 recognizes the Summit48si DC power supply, but does not indicate the type of PSU installed, issue a warning if both an AC and a DC PSU are installed in the same chassis, or send an SNMP trap message when the PSU is hot-swapped.

GBIC Support

GBICs supported with ExtremeWare 7.2.0b37, and the minimum ExtremeWare version required, include:

Table 5: GBIC support

GBIC	ExtremeWare Required
SX parallel ID	1.0
SX serial ID	2.0

Table 5: GBIC support

GBIC	ExtremeWare Required
LX parallel ID	1.0
LX serial ID	2.0
ZX	6.2.2
ZX Rev 03	6.2.2
LX70	2.0
LX100	6.1.9
UTP	6.1.9
SX Mini	7.0.1b11
LX Mini	7.0.1b11
ZX Mini	7.0.1b11

The following table describes how each version of ExtremeWare interprets the media type of the installed GBIC, based on either the Vista web interface, or the `show port configuration` command. All versions correctly identify Parallel ID GBIC types; however, some versions do not correctly identify the Serial ID GBIC type because the Serial ID GBICs were introduced after the software was released.

Table 6: ExtremeWare recognition of GBIC type

ExtremeWare Version	SX Parallel ID	LX Parallel ID	SX Serial ID	LX Serial ID	LX70
1.x	SX	LX	Not Supported	Not Supported	Not Supported
2.x	SX	LX	LX	LX	LX
3.x	SX	LX	CX	CX	CX
4.x	SX	LX	SX	LX	LX
6.x	SX	LX	SX	LX	LX70 (6.1.6 and above)
7.x	SX	LX	SX	LX	LX70

Mini-GBIC Support

Extreme products support the Extreme mini-GBIC only. For reliability and stability reasons, third-party mini-GBICs are not supported at this time.

XENPAK Module Support

XENPAK modules supported with ExtremeWare 7.2.0b37, the minimum ExtremeWare version required, and the manufacturers supported include:

Table 7: XENPAK support

XENPAK Module	ExtremeWare Required	Manufacturers Supported
LR	7.2.0b18	Intel, Opnext
ER	7.2.0b18	Intel, Opnext

2 Upgrading to ExtremeWare 7.2

This chapter contains the following sections:

- Staying Current on page 21
- Upgrading ExtremeWare on page 21
- Downgrading Switches on page 27

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site:

http://www.extremenetworks.com/go/esupport.htm.

Upgrading ExtremeWare

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2b56 (or later). You can only load ExtremeWare 6.2.2 on a switch running ExtremeWare 6.1.9 (or later). Table 8 lists the BootROM required for each version of ExtremeWare.

Table 8: Required BootROM versions

ExtremeWare Version	BootRom Version
ExtremeWare 7.1.1 and later	BootROM 8.1 (or later)
ExtremeWare 7.0.0 through ExtremeWare 7.1.0	BootROM 7.8 (or later)
ExtremeWare 6.2.2 through ExtremeWare 6.2.2	BootROM 7.8
ExtremeWare 6.2.2 through ExtremeWare 6.2.2	BootROM 7.6 (or later)
ExtremeWare 6.1.8 through ExtremeWare 6.2.1	BootROM 7.2 (or later)
ExtremeWare 6.1 through ExtremeWare 6.1.7	BootROM 6.5

If your switch is running ExtremeWare 6.1.8 (or earlier), you must first upgrade to ExtremeWare 6.1.9, then upgrade to ExtremeWare 6.2.2b56 (or later). Following are specific instructions on upgrading to, and downgrading from, ExtremeWare 7.2.0b37 for Summit, Alpine, and BlackDiamond switches.

Upgrading Switches to ExtremeWare 7.2.0

To install ExtremeWare 7.2.0b37, you must:

1. Save the configuration to a TFTP server.
2. Upgrade the BootROM to Version 8.1 as described on page 23.
3. Upgrade to ExtremeWare 6.1.9 as described on page 23.
4. Upgrade to ExtremeWare 6.2.2b56 as described on page 23.
5. Upgrade to ExtremeWare 7.2.0b37 as described on page 24.
6. Upgrade T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79 as described on page 25.
7. Upgrade T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later as described on page 26.
8. Upgrade ATM, MPLS, ARM, or PoS Modules from a Release Prior to ExtremeWare 6.1.8b79 as described on page 26.

If you have already installed ExtremeWare 6.1.9 through ExtremeWare 6.2.2b43, you can skip step 3. If you have already installed ExtremeWare 6.2.2b56 through ExtremeWare 7.0.1, you can skip steps 3 and 4.

NOTE

If you are also upgrading your BlackDiamond to MSM-3's, see the MSM-3 Upgrade Note *included with your MSM-3.*

NOTE

The Alpine 3802 requires a different upgrade procedure, described on page 27.

Save the Current Configuration

Before upgrading ExtremeWare, save your configuration using the following steps. This preserves the ability to downgrade should it become necessary.

1. If you are using the Network Login campus mode:
   a. Disable Network Login using the `disable netlogin` command to prevent users from re-authenticating during the backup process.
   b. Use the `clear netlogin state port` command on all Network Login user ports, causing all Network Login users to be unauthenticated and all client ports to move back to their respective unauthenticated VLAN configuration.
   c. Use the `show netlogin` and `show vlan` commands to verify that all Network Login ports are in the unauthenticated state and the client ports are members of their respective unauthenticated VLANs.
2. If you are using ACLs and the CPU DoS protect feature, ensure that the CPU DoS protect filter precedence follows the rules described in "CPU DoS Protect and ACL Precedence" on page 54. If there is a precedence conflict, CPU DoS protect is not enabled.
3. Save the current configuration in both the primary and secondary configuration spaces using the `save configuration primary` and `save configuration secondary` commands.

4 Configure the switch to use the primary image and the primary configuration using the `use image primary` and `use configuration primary` commands.

5 Verify that all of the above procedures were completed successfully with the `show switch` command.

6 Upload the configuration to a TFTP server for safekeeping using the `upload configuration` command.

Upgrade the BootROM to Version 8.1

Before you upgrade ExtremeWare, upgrade to BootROM 8.1 (BootROM 8.1 is compatible with all ExtremeWare versions back to ExtremeWare 6.1.9):

1 Download the BootROM using the `download bootrom [<host_name> | <ip_addr>] <ngboot.bin_name>` command.

2 Reboot the switch using the `reboot` command.

Upgrade to ExtremeWare 6.1.9

If you are running ExtremeWare 6.1.8 (or earlier), upgrade to ExtremeWare 6.1.9:

1 TFTP download ExtremeWare 6.1.9 to the primary image space using the `download image primary` command.

CAUTION

If you do not upgrade to ExtremeWare 6.1.9 before downloading ExtremeWare 6.2.2, the ExtremeWare 6.2.2 download will fail, and the following message will be printed from the system:

```
ERROR: File too large
```

2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 Check the log for configuration errors. Manually enter configurations that did not load.

5 If you configured Random Early Drop Probability in ExtremeWare 6.1.8 (or earlier), re-configure the Random Early Drop Probability using the `configure red drop-probability` command.

6 Save the configuration to the primary space.

Upgrade to ExtremeWare 6.2.2b56

If you are running ExtremeWare 6.1.9 to ExtremeWare 6.2.2b43, upgrade to ExtremeWare 6.2.2b56 (you can substitute ExtremeWare 6.2.2 builds 68, 108, 124, 134, and 156 for build 56):

1 TFTP download ExtremeWare 6.2.2b56 to the primary image space using the `download image primary` command.

2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

NOTE

ExtremeWare 6.2.2b56 (and later) stores 75 static log entries. Previous versions stored 100 entries. To accommodate the new entry limit, ExtremeWare 6.2.2b56 clears the static log after your first reboot. To preserve your static log entries, use the `show log` *command and save the output.*

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 TFTP download the saved configuration, and answer `y` at the prompt to reboot the switch.

5 Check the log for configuration errors. Manually enter configurations that did not load.

6 Save the configuration.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

NOTE

After upgrading from ExtremeWare 6.1.9 to ExtremeWare 6.2.2, the IGMP snooping leave time-out value will be changed from 10 seconds to 0. This results in an IGMP snooping membership entry being removed immediately when an IGMP leave is received from a host.

This is good for an environment where only one host is connected. Use the `configure igmp snooping leave-timeout` *command to change the leave time-out value back to 10 seconds.*

Upgrade to ExtremeWare 7.2.0b37

If you are running any software image from ExtremeWare 6.2.2b56 to ExtremeWare 7.1.1 (or later), upgrade to ExtremeWare 7.2.0b37:

NOTE

If you are upgrading a chassis with MSM64i's to MSM-3's, see the MSM-3 Upgrade Note included with your MSM-3.

1 Upload the configuration to your TFTP server using the `upload configuration` command.

2 Clear your switch using the `unconfigure switch all` command, and enter `y` at the prompt to reboot the switch. If you started the upgrade process with ExtremeWare 6.2.2b56 or later, you can skip this step.

3 TFTP download ExtremeWare 7.2.0b37 to the primary image space using the `download image primary` command.

4 Reboot the switch using the `reboot` command.

NOTE

If you have Hitless Failover enabled on your MSM-3, you can use the hitless upgrade procedure.

5 Verify that the correct ExtremeWare version is loaded on the switch using the `show switch` command.

6 TFTP download the configuration you saved in Step 1, and enter `y` at the prompt to reboot the switch.

NOTE

If you are using EAPS and are upgrading from a version prior to ExtremeWare 6.2.2b134 or from ExtremeWare 7.0, the default failtimer expiry action changes to sending an alert. This keeps your ring from failing over when there is no break in the ring, such as in the event of a broadcast storm, busy CPU, or misconfigured control VLAN. To change the failtimer expiry action to opening the secondary port, especially if your EAPS traffic flows through switches that do not support EAPS, use the configure eaps failtime expiry-action command.

7 Check the log for configuration errors. Manually enter configurations that did not load.

8 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

9 If you are upgrading a BlackDiamond switch, synchronize the BootROM, image, and configuration across all installed MSM modules using the `synchronize` command. This command reboots the synchronized modules.

You can ignore any diagnostics failure messages generated by the synchronization.

10 Reboot the switch using the `reboot` command.

11 If you are using the Network Login campus mode:

a Manually enable Network Login using the `enable netlogin [web-based | dot1x]` command.

b Verify that users are able to authenticate and successfully access network resources.

Upgrade T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79

If you are using a T1, E1, or T3 module with an ExtremeWare release prior to 6.1.8b79 or a BootROM prior to 2.8, upgrade the module to ExtremeWare 7.2.0b37:

1 TFTP download ExtremeWare 6.1.8b79 for the module using the `download image slot primary` command.

NOTE

T1, E1, and T3 modules must be using ExtremeWare 6.1.8b79 and BootROM 2.8 before upgrading to ExtremeWare 7.2.0b37.

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 3 until you have upgraded every module, then reboot the switch instead of rebooting each slot.

4 Verify that the correct ExtremeWare is loaded using the `show version` command. You should see output similar to the following:

```
BootROM: 251.251
Image: WM4T1 Version 6.1.8 (Build 79)
```

If you see a version other than Build 79, repeat steps 1 - 4.

5 Download the BootROM using the `download bootrom slot` command.

6 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 6, upgrade every module, then reboot the switch.

7 Download the latest ExtremeWare to the primary image space.

8 Reboot the module using the `reboot slot` command.

Upgrade T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later

If you are using a T1, E1, or T3 module with ExtremeWare 6.1.8b79 (or later) and BootROM 2.8 (or later), upgrade the module to ExtremeWare 7.2.0b37:

1 TFTP download the latest ExtremeWare for the module using the `download image slot primary` command.

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

Upgrade ATM, MPLS, ARM, or PoS Modules from a Release Prior to ExtremeWare 6.1.8b79

If you are using an ATM, MPLS, ARM, or PoS module with an ExtremeWare release prior to 6.1.8b79 or a BootROM prior to 1.18, upgrade the module to ExtremeWare 7.2.0b37:

1 TFTP download ExtremeWare 6.1.8b79 for the module using the `download image slot primary` command.

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 3 until you have upgraded every module, then reboot the switch instead of rebooting each slot.

4 Verify that the correct ExtremeWare is loaded using the `show version` command.

5 Download the BootROM using the `download bootrom slot` command.

6 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 6, upgrade every module, then reboot the switch.

7 Download the latest ExtremeWare to the primary image space.

8 Reboot the module using the `reboot slot` command.

Upgrading an Alpine 3802 to ExtremeWare 7.2.0b37

To upgrade an Alpine 3802 to ExtremeWare 7.2.0b37:

1. Upload the configuration to your TFTP server using the `upload configuration` command.
2. Upgrade to BootROM 8.1 using the `download bootrom` command.
3. Reboot the switch using the `reboot` command.
4. TFTP download ExtremeWare 6.1.8w3.0.1 b79 to the primary image space using the `download image primary` command.
5. Verify that the correct BootROM and ExtremeWare versions are loaded on the switch using the `show switch` and `show version` commands.
6. Answer `y` at the prompt to reboot the switch.
7. TFTP download ExtremeWare 7.0.0b46 to the primary image space using the `download image primary` command.
8. Reboot the switch using the `reboot` command.
9. TFTP download the latest ExtremeWare 7.2.0b37 build to the primary image space using the `download image primary` command.
10. Reboot the switch using the `reboot` command.
11. TFTP download the configuration you saved in Step 1, and enter `y` to reboot the switch.
12. Check the log for configuration errors. Manually enter configurations that did not load.
13. Save the new configuration to the primary space.

    Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

Downgrading Switches

Assuming that the previous configuration is in the secondary configuration space and the previous image is in the secondary image space:

1. If you saved an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, configure the switch to use that configuration with the `use configuration secondary` command.

   If you did not save an earlier configuration, re-configure the switch or download a configuration at the end of this process.
2. If you did not save the earlier ExtremeWare image in the secondary image space, download the image using the `download image secondary` command.

   NOTE

   If you downgrade to an ExtremeWare version that does not support software signatures (ExtremeWare 6.2.2b56 or later supports software signatures), you must follow the upgrade procedures in the preceding sections to get back to ExtremeWare 7.2.0b37. You cannot switch between primary and secondary images on the switch unless they both support software signatures.
3. Use the image in the secondary image space with the `use image secondary` command.
4. Verify that the above procedures were completed successfully with the `show switch` command.

5 Downgrade to the appropriate BootROM version. The `show version` command displays the BootROM version as "Unknown" when the BootROM is downgraded.

6 Reboot the switch.

NOTE

When downgrading to a previous version of ExtremeWare, ensure that the switch configuration matches that version of ExtremeWare or below. Pointing the configuration to a new version of ExtremeWare and using a previous version of ExtremeWare is not supported. You will get a warning message from the system when attempting to do so.

7 If you did not save an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, re-configure the switch or download a configuration.

3 Supported Limits

This chapter summarizes the supported limits in ExtremeWare.

Supported Limits

The table below summarizes tested metrics for a variety of features. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeWare Software User Guide*.

Table 9: Supported limits

Metric	Description	Limit
Access List rules	Maximum number of Access Lists (best case).	5120
Access List rules—BlackDiamond 6816	Maximum number of BlackDiamond 6816 Access Lists (best case).	3500
Access List rules—Summit	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255
Access List rules—Alpine	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255
Access List rules—BlackDiamond	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255 per I/O module
Access Profiles	Maximum number of access profiles per switch.	128
Access Profile entries	Maximum number of access profile entries per switch.	256
Application Examination rules	Maximum number of Application Examination rules.	1000
Application Examination rules/port	Maximum number of Application Examination rules per port.	60
BGP—Peer Groups	Maximum number of BGP peer groups per switch.	16
BGP—peers	Maximum number of BGP peers per switch.	200
BGP—routes, MSM-3	Maximum number of routes received and contained in the BGP route table (best case).	2,625,000
BGP—routes, MSM64i, Summit7i, Alpine	Maximum number of routes received and contained in the BGP route table (best case).	1,275,000

Table 9: Supported limits (continued)

Metric	Description	Limit
BGP—routes, Summit1i, Summit5i, Summit48i, Summit48si	Maximum number of routes received and contained in the BGP route table (best case).	180,000
BGP—NLRI filters	Maximum number of NLRI filters per switch.	128
BGP—NLRI filer add entries	Maximum number of NLRI add entries per switch.	256
BGP—AS-Path filters	Maximum number of AS-Path filters per switch.	128
BGP—AS-Path filter add entries	Maximum number of AS-Path filter add entries per switch.	256
BGP—network statements	Maximum number of network statements per switch.	256
BGP—aggregate addresses	Maximum number of aggregate routes that can be originated per switch.	256
Jumbo Frame size	Maximum size supported for Jumbo frames, including the CRC.	9216
EAPS—Domains/switch	Maximum number of EAPS domains.	64
EAPS—Domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	64
EAPS—VLAN links	Maximum number of Control or Protected VLANs per EAPS domain.	4093
EAPS—Bridge links	Maximum number of EAPS bridge links per switch.	4096
EAPS—Master nodes	Number of Master nodes per EAPS domain.	1
EAPS—Switches	Maximum number of EAPS switches per ring.	No limit
EMISTP & PVST+ — maximum domains, Summit	Maximum number of EMISTP and PVST+ domains.	128
EMISTP & PVST+ — maximum domains, Alpine	Maximum number of EMISTP and PVST+ domains.	256
EMISTP & PVST+ — maximum domains, BlackDiamond	Maximum number of EMISTP and PVST+ domains.	512
EMISTP & PVST+ — maximum ports	Maximum number of EMISTP and PVST+ ports.	3840
EMISTP & PVST+ — maximum domains per port, Summit	Maximum number of EMISTP and PVST+ domains that can be configured per port.	128
EMISTP & PVST+ — maximum domains per port, Alpine	Maximum number of EMISTP and PVST+ domains that can be configured per port.	256
EMISTP & PVST+ — maximum domains per port, BlackDiamond	Maximum number of EMISTP and PVST+ domains that can be configured per port.	512
ESRP—maximum domains	Maximum number of ESRP domains for a single switch.	64
ESRP—maximum instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—maximum ESRP groups	Maximum number of ESRP groups within a broadcast domain.	4
ESRP—maximum ESRP groups with bi-directional rate shaping	Maximum number of ESRP groups within a broadcast domain when bi-directional rate shaping is enabled.	3
ESRP—maximum VLANs in a single ESRP domain – Summit, Alpine	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	256 recommended; 3000 max

Table 9: Supported limits (continued)

Metric	Description	Limit
ESRP—number of VLANs in a single ESRP domain, BlackDiamond	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	1024 recommended; 3000 max
ESRP—Route-track entries, Summit, Alpine, BlackDiamond	Maximum number of routes that can be tracked for each ESRP domain.	4
ESRP—maximum VLAN tracks	Maximum numbers of VLAN tracks per VLAN.	1
FDB—maximum ports for permanent entries	Maximum number of ports supported for permanent FDB entries.	2,000
FDB—maximum L2/L3 entries – BlackDiamond, Summit5i, Summit7i, Alpine 3804, Alpine 3808	Maximum number of MAC addresses/IP host routes for the MSM64i, Summit5i, Summit7i, Alpine 3804, and Alpine 3808.	262,144
FDB—maximum L2/L3 entries – Summit1i, Summit48i, Summit48si, Alpine 3802	Maximum number of MAC addresses/IP host routes for the Summit1i, Summit48i, Summit48si, and Alpine 3802.	131,072
Flow Redirection—maximum redirection rules	Maximum number of rules that can point to the same or separate groups of web cache servers.	64 (8 servers is the maximum)
Flow Redirection—maximum enumeration mode entries	Maximum number of active entries for enumeration mode rules. For example, one /16 rule can take all of the available entries.	64,000
Flow Redirection—maximum subnet mode entries	Maximum number of active entries for subnet mode rules. Each mask can have 1 entry.	64
IP ARP entries	Maximum number of IPARP entries.	20,480
IP ARP Static entries	Maximum number of permanent IP static ARP entries supported.	512
IP ARP Static Proxy entries	Maximum number of permanent IP ARP proxy entries.	512
IP Route Sharing Entries (ECMP)—static or OSPF	Maximum number of static or OSPF routes used in route sharing calculations.	12
IP Route Sharing Entries (ECMP)—IS-IS	Maximum number of IS-IS routes used in route sharing calculations.	8
IP Router interfaces	Maximum number of VLANs performing IP routing - excludes SubVLANs.	512
IP Static Routes	Maximum number of permanent IP routes.	1024
IPX Static Routes and Services (RIP and SAP)	Maximum number of static IPX RIP route and IPX SAP entries.	64 for each
IPX dynamic routes and services	Maximum recommended number of dynamically learned IPX RIP routes and SAP entries.	2000 for each
IPX Router interfaces	Maximum number of IPX router interfaces.	256
IPX Access control lists	Maximum number of Access Lists in which all rules utilize all available options.	worst case: 255
IS-IS—maximum routing interfaces	Maximum IS-IS routing interfaces.	255
IS-IS—maximum routes	Maximum IS-IS routes.	25,000
IS-IS—maximum adjacencies	Maximum IS-IS adjacencies per routing interface.	64
IS-IS—maximum domain summary addresses	Maximum IS-IS domain summary addresses.	32
IS-IS—maximum redistributed routes, regular metric	Maximum IS-IS redistributed routes using the regular metric.	20,000

Table 9: Supported limits (continued)

Metric	Description	Limit
IS-IS—maximum redistributed routes, wide metric	Maximum IS-IS redistributed routes using the wide metric.	30,000
IS-IS—maximum redistributed routes, both metrics	Maximum IS-IS redistributed routes using both metrics.	10,000
Logged Messages	Maximum number of messages logged locally on the system.	20,000
MAC-based VLANs—MAC addresses	Maximum number of MAC addresses that can be downloaded to the switch when using MAC-based VLANs.	7000
MAC-based security	Maximum number of MAC-based security policies.	1024
Mirroring—mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8
Mirroring—number of VLANs	Maximum number of VLANs that can be mirrored to the mirror port.	8
NAT—maximum connections	Maximum number of simultaneous connections per switch.	256,000
NAT—maximum rules	Maximum number of rules per switch.	2048
NAT—maximum VLANs	Maximum number of inside or outside VLANs per switch.	The switch's limit
NetFlow—Filters	Maximum number of NetFlow filters in a switch.	128
NetFlow—Groups	Maximum number of NetFlow groups.	32
NetFlow—Hosts	Maximum number of NetFlow hosts.	8/group
Network Login—Maximum clients	Maximum number of Network Login clients per switch.	1024
Network Login—802.1x	Maximum recommended Session-Timeout value returned by RADIUS server.	7200 seconds
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF external routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	130,000
OSPF inter- or intra-area routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	16,000
OSPF external routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	65,000
OSPF inter- or intra-area routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	8,000
OSPF routers in a single area	Recommended maximum number of routers in a single OSPF area.	200
OSPF interfaces on a single router	Recommended maximum number of OSPF routed interfaces on a switch.	384
OSPF virtual links	Maximum number of OSPF virtual links supported.	32

Table 9: Supported limits (continued)

Metric	Description	Limit
OSPF adjacencies—Summit1i, Summit5i, Summit48i, Summit48si	Maximum number of OSPF adjacencies on a switch with 128 MB memory.	150
OSPF adjacencies—Summit7i, Alpine, BlackDiamond	Maximum number of OSPF adjacencies on a switch with 256 MB memory.	225
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	384
Route Maps	Maximum number of route maps supported on a switch.	128
Route Map Entries	Maximum number of route map entries supported on a switch.	256
Route Map Statements	Maximum number of route map statements supported on a switch.	512
SLB—maximum number of simultaneous sessions	For Transparent and Translational and GoGo modes respectively.	500,000/500,000/ unlimited
SLB—maximum number of VIPs	For Transparent and Translational and GoGo modes respectively.	1000/1000/unlimited
SLB—maximum number of Pools	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of Nodes per Pool	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of physical servers per group	Applies to GoGo mode only; a group shares any number of common VIPs.	8
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—Trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—Users	Maximum number of SNMPv3 users.	32
SNMPv3—Groups	Maximum number of SNMPv3 groups.	64
SNMPv3—Accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—Communities	Maximum number of SNMPv3 communities.	64
SNMPv3—Target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—Target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—Notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—Filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—Filters	Maximum number of SNMPv3 notify filters.	400
Spanning Tree—maximum STPDs, Summit	Maximum number of Spanning Tree Domains.	128
Spanning Tree—maximum STPDs, Alpine	Maximum number of Spanning Tree Domains.	256
Spanning Tree—maximum STPDs, BlackDiamond	Maximum number of Spanning Tree Domains.	512
Spanning Tree—minimum STPDs	Minimum number of Spanning Tree Domains.	1
Spanning Tree—802.1d domains	Maximum number of 802.1d domains per port.	1

Table 9: Supported limits (continued)

Metric	Description	Limit
Spanning Tree—number of ports	Maximum number of ports that can participate in a single Spanning Tree Domain.	4096
Spanning Tree—minimum number of ports	Minimum number of ports that can participate in a single Spanning Tree Domain.	1
Spanning Tree—minimum number of domains/port	Minimum number of Spanning Tree Domains that can be configured per port.	1 for default VLAN, 0 for others
Spanning Tree—Spanning Tree modes	Maximum number of Spanning Tree modes per switch.	2 (dot1d and dot1w)
Static MAC FDB entries—Summit, Alpine, BlackDiamond	Maximum number of permanent MAC entries configured into the FDB.	2000
Super-VLAN—number of ports & sub-VLANs	Maximum number of ports and sub-VLANs associated with each super-VLAN.	2550
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
UDP profiles	Number of profiles that can be created for UDP forwarding.	10
UDP profile entries	Number of entries within a single UDP profile.	16
VLANs—Summit, Alpine	Includes all VLANs plus sub VLANs, super VLANs, etc.	4095
VLANs—BlackDiamond 6816 fully populated	Includes all VLANs plus sub VLANs, super VLANs, etc.	681
VLANs—BlackDiamond 6816 with up to 7 I/O modules	Includes all VLANs plus sub VLANs, super VLANs, etc.	1776
VLANs—BlackDiamond	Includes all VLANs plus sub VLANs, super VLANs, etc.	4095
VLANs—maximum active protocol-sensitive filters	The number of simultaneously active protocol filters in the switch.	15
VRRP—maximum VRIDs	Maximum number of unique VRID numbers per switch.	4
VRRP—maximum VRIDs with bi-directional rate shaping	Maximum number of unique VRID numbers per switch when bi-directional rate shaping is enabled.	3
VRRP—maximum VLANs/switch	Maximum number of VLANs per switch.	64
VRRP—maximum VRIDs/VLAN	Maximum number of VRIDs per VLAN.	4
VRRP—maximum ping tracks	Maximum number of ping tracks per VLAN.	4
VRRP—maximum iproute tracks	Maximum number of iproute tracks per VLAN.	4
VRRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1

4 Clarifications, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification, behaviors that might not be intuitive, and issues that have been resolved since the last release. Numbers in parentheses are for internal reference and can be ignored.

This chapter contains the following sections:

- Clarifications and Known Behaviors on page 35
- Issues Resolved in ExtremeWare 7.2.0b37 on page 60
- Issues Resolved in ExtremeWare 7.2.0b33 on page 61
- Issues Resolved in ExtremeWare 7.2.0b25 on page 66
- Issues Resolved in ExtremeWare 7.2.0b18 on page 68

Clarifications and Known Behaviors

Following are the clarifications and known behaviors in ExtremeWare 7.2.0b37. For changes made in previous releases, see the release notes specific to the release.

General

Changing Port Speed Stops Packet Transmission

Changing the port speed on a Fast Ethernet port sending L2 traffic with auto negotiation set to off stops packets from being received on one end of a bidirectional switch configuration (PD2-216008619).

Creating an ACL with a Filter-Precedence Generates a Conflict Error

When enabling cpu-dos-protect on the switch, a filter-precedence of 10 (default) is used. If you configure another ACL with a filter-precedence of 11 and 12, a conflict error with CPU DOS Protection is generated (PD3-11296780, PD2-241094151, PD2-241094160).

Error Message While Hot-Removing Line Cards

If you hot-remove a G8Xi blade, the following error message may be generated in the syslog:

```
<Crit:SYST> Failed in fdbHwNgInitMc
```

This error message is generated when the switch has approximately 64K L2 FDB entries with traffic running (PD3-817627).

System Related – All Systems

Autonegotiation Setting Not Preserved on Added and Deleted Loopback Ports

If you add a 10/100 port as a loopback port and delete it, autonegotiation is set to off (PD2-192574401).

The show log Command Truncates Long Commands

If you download a configuration, the output of the `show log` command might not completely display commands longer than 240 characters. This is a display problem; the configuration loads correctly (PD2-171470611).

The show log Display Truncates Configuration Parsing

If you download a configuration and use the `show log` command to view the parsing of the configuration, the log does not display the entire parsing. This is a display problem; the configuration parses and loads correctly (PD2-171470601).

Do Not Create Single-Character Names

When you create named components such as VLAN or access group names, do not use single character names. The single character might be interpreted by the switch as a truncated parameter. For example, if you name an SNMPv3 access group "a" and delete that access group using the `configure snmpv3 delete access a` command, the switch might interpret the command as `configure snmpv3 delete access all-non-default` (PD2-152594408).

Telnet and the show ports Command

If you telnet to the switch and use the `show ports info detail` command, the line feeds might not be recognized, resulting in output lines overwriting previous lines (PD2-130127501).

The show configuration Output

After using the `unconfigure switch all` command, the `show configuration` output displays the VLAN *default* without any ports assigned. The ports still belong to the VLAN *default*, as the `show vlan` output correctly displays (PD2-128233941).

LACP not Supported

Contrary to the information in the *ExtremeWare 7.2 Software User Guide* and *ExtremeWare 7.2 Command Reference Guide*, LACP is not supported.

Upgrading to ExtremeWare 7.0 and Bi-Directional Rate Shaping

When you directly upgrade from ExtremeWare 6.2.2 to ExtremeWare 7.0 (or later), bi-directional rate shaping does not work if the loopback ports were in autonegotiation mode. This behavior is not displayed by 10/100Base-T or Gigabit fiber ports. A workaround is to remove and re-add the loopback ports to the VLAN (PD2-107820904).

Upgrading to ExtremeWare 7.0 and OSPF

If you upgrade directly from ExtremeWare 6.2.2 to ExtremeWare 7.0 (or later), the OSPF metric for 10 Gigabit interfaces is incorrect. A workaround is to manually configure the OSPF metrics, or to upload the configuration before upgrading and then download the ExtremeWare 6.2.2 configuration (PD2-108161623).

Blank Space in show port info detail Command Output

The output of the `show port info detail` command contains several blank pages. The output still contains all of the requested information (PD2-107800978).

Using an ExtremeWare 7.0 Configuration with an Earlier Image

If you are using an ExtremeWare 7.0 (or later) configuration and attempt to use an earlier image, the switch prompts you for confirmation (because this combination is not recommended). If you answer "`n`" at the prompt, you receive the following error message:

```
Error: bad image.
```

You can safely ignore this message (PD2-110983501).

Console Response with a Large Number of ARP Entries

Console response is slow when the switch is learning 10,000 or more ARP entries. This does not affect performance. Console response returns to normal when the entries are learned (PD2-104103941).

The show log chronological Command

When the syslog contains more than 1,000 lines, the `show log chronological` command displays nothing. However, the command `show log` displays correctly (PD2-104062736).

BOOTP-Dependent Routes in Downloaded Configuration not Created

Static and default routes that depend on a BOOTP IP address/subnet are not created when you download a configuration (PD2-86888351).

BlackDiamond

Changing Address-Based Algorithms to L2_L3 Does Not Preserve After Save and Reboot

When you configure load sharing and set the sharing algorthim to address-based L2_L3, save the configuration, and reboot the switch, the load sharing configuration setting is not preserved after the reboot (PD2-243743150).

Cross-Module Trunking and Hitless Failover

For traffic load-shared across I/O modules, failover is not hitless; traffic loss occurs for approximately four seconds (PD2-186133901).

Autonegotiation Off Command Accepted on 10 Gigabit Ethernet Modules

Although you cannot disable autonegotiation on the 10 Gigabit Ethernet modules, the command to turn off autoneogtiation is accepted and the resulting display shows autonegotiation status as off (PD2-223283401).

Disabling One MSM Might Cause Loss of Throughput

If you disable one MSM in a dual-MSM configuration, you might lose half of the throughput on ARM and MPLS modules (PD2-199171610).

The output of the `show diagnostics backplane utilities` command shows slots with ARM or MPLS modules as having only two backplane links, rather than the normal four backplane links.

Cannot Delete an LSP Previously Referenced by a TLS Tunnel

You cannot delete an LSP previously referenced by a TLS tunnel. To delete the LSP, first reboot the switch (PD2-222522101).

10 Gigabit Ethernet and CMT

If you use 10GLRi or XENPAK ports with the address-based or round robin load-sharing algorithms and the master link is lost, FDB entries are not learned (PD2-197753713).

XENPAK with the BlackDiamond 6816

On a BlackDiamond 6816, if you configure the MSM to keep links up, save the configuration, and reboot the switch, XENPAK links do not come up (PD2-198280301).

Cross-Module Trunking Not Supported on MSM64i's

If you enable cross-module trunking on a chassis with MSM64i's installed, you receive the following error message:

```
All load share ports must be on the same module
```

Cross-module trunking is not supported with MSM64i's. To enable load sharing across modules, install MSM-3's (PD2-193845958).

Cross-Module Trunking Module Support

Table 10 lists the modules that support load-sharing across modules.

Table 10: Cross-module trunking module support

Module	CMT Support
G8Xi	Yes
G8Ti	Yes

Table 10: Cross-module trunking module support (continued)

Module	CMT Support
G12SXi	Yes
G16X[3]	Yes
G24T[3]	Yes
F32Fi	Yes
F48Ti	Yes
F96Ti	Yes
WDMi	No
10GLRi	Yes
10GX3	Yes
MPLS	No
ARM	No
P3cMi	No
P3cSi	No
P12cMi	No
P12cSi	No
A3cMi	No
A3cSi	No

Cross module trunking is not supported on WDMi modules (PD2-176314520).

Master Slot Must Be Active for CMT

The slot with the master load-sharing port must be populated and active when you configure a cross-module load-sharing group. If the master slot is unavailable at configuration, cross-module load-sharing traffic is not forwarded (PD2-175825901, PD2-175854401).

MSM-3 Log Might Be Out of Chronological Order

Log events are stored independently on the master and slave MSM-3. Thus, a failover might cause the log to appear out of chronological order, or missing information. Concatenating the logs provides all log information (PD2-172852704).

Source Addresses Might Age Out of FDB

If a MAC source address is exclusively sourced on a slave CMT slot, such as with a port-based algorithm, the FDB entry might be aged out. To avoid this, use address-based load sharing on the neighbor switch (PD2-170942776).

Do Not Use Static FDB Entries with CMT

Do not use static FDB entries with CMT. If the CMT master fails, static FDB entries are not transferred to the group members (PD2-170942732, PD2-170942701).

Saving Health Check Configuration After Failure Causes Console Crash

If an MSM fails a system health check with packet memory errors and is taken offline, the slave becomes the master, but you cannot save the configuration. To avoid this, clear the diagnostics, upload the configuration, and reboot the switch before saving (PD2-171914501).

Diagnostics on MSM-3 with Hitless Failover Causes Failover and Spurious Message

Running diagnostics on the master MSM-3 with hitless failover enabled causes the MSM-3 to fail over to the slave and log a hardware failure message. You can safely ignore this message (PD2-168317013).

Do Not Configure a Port-Based Backplane Algorithm When CMT is Enabled

Do not configure a port-based backplane policy when CMT is enabled. It might cause all egress ports on a given slot to be skipped. To work around this problem, configure an address-based backplane policy. In a similar manner, if a port-based algorithm is selected for the trunk, some egress ports might be skipped. To change the load share policy of a trunk, disable sharing for the port and enable sharing with an address-based policy, then reboot the switch (PD2-165883601).

Cross-Module Trunking and ACLs

Flooding on a CMT trunk cannot initially be blocked by ACLs. After the remote end responds with a PDU, the destination address is learned via source address learning. Once the address is learned, packets are blocked in hardware by an ACL (PD2-153404501, PD2-115139620, PD2-130299801, PD2-130299807).

4,000 VLANs on a BlackDiamond

If you configure more than 4,000 VLANs, EDP might crash, causing ESRP to fail (PD2-153821210).

PPP Links Through E1 modules

PPP links through the E1 module are not always re-established after a reboot. To re-establish the PPP link, use the `restart ports` command (PD2-109252301).

Slot Failure Messages During a Broadcast Storm

If you have more than 15 Gigabit Ethernet links between two chassis, all in the same VLAN and generating a broadcast storm, the system health check records slot failures in the log. When the broadcast storm stops, the log messages also stop (PD2-117946811).

No Image Information Reported to SNMP with One MSM

If you only install an MSM in slot B of a BlackDiamond 6804, BlackDiamond 6808, or BlackDiamond 6816, no primary or secondary image information is reported to your SNMP NMS (PD2-129612901).

BlackDiamond 6816 MSM C and D Diagnostics Messages not in Syslog

If you run diagnostics on an MSM in slot C or D of a BlackDiamond 6816, messages are not recorded in the syslog. To view the diagnostics messages, use the `show diagnostics` command (PD2-118049501).

Disabling CLI Paging from the Slave MSM64i

Enabling or disabling CLI paging from the slave MSM64i has no affect on the master MSM64i paging configuration (PD2-104377501).

The unconfig switch all Command

If you use the `unconfig switch all` command and immediately use the `config default vlan delete port all` command, the switch reboots. To avoid this situation, after you unconfigure the switch, wait for the switch to completely reboot before you delete the ports (PD2-105474401).

BlackDiamond 6816 MIB Value for Input Power Voltage

On the BlackDiamond 6816, the extremeInputPowerVoltage attribute in extremeSytemCommonInfo is shown as "0" and the extremePowerSupplyInputVoltage in the extremePowerSupplyTable is shown as "unknown." These values cannot be obtained from the switch (1-841J1).

Alpine

Mirroring Failure on an Alpine3808 with GM4x Card After a Save and Reboot

Port mirroring may fail on the Alpine3808 with a Gigabit Ethernet, 4-port, GBIC module after saving and rebooting the switch. The displayVpst for the ports after rebooting the switch indicates that the mirroring flag is not set after the reboot even though the configuration has been saved. As a workaround, disable and enable the mirroring port and reboot the switch (PD3-1025737).

Logs with attachment.Autonegotiation on VDSL Ports Set Incorrect Speed

A VDSL port configured to autonegotiate sets the speed to 100 Mbps when connected to a 100 Mbps port. The maximum speed for the VDSL port is 10 Mbps. As a workaround, configure autonegotiation off, and set the speed to 10 Mbps, full duplex. For example, to configure port 3:1, use the following command:

```
configure port 3:1 auto off speed 10 duplex full
```

(PD2-209953030)

VDSL Ports do not Support Jumbo Frames

Do not enable jumbo frames on VDSL ports. Jumbo frames are not supported on VDSL ports (PD2-208090059).

Status LED Solid After Fan Tray Reseated

If you reseat the fan tray in an Alpine 3804 or Alpine 3808, the status LED on the SMMi is solid green. The LED should blink. The LED does not blink correctly until you reboot the switch (PD2-205947223).

New Accounts with WAN Module Installed are pppuser

If you have a WAN module installed and you create a user account, the account is automatically created as pppuser (PD2-197374626).

Traffic Diagnostics Not Performed During Extended Diagnostics on T1 Module

If you run extended diagnostics on a T1 module, T1 traffic diagnostics are not performed (PD2-187132901).

Traffic Diagnostics Not Performed During Extended Diagnostics on E1 Module

If you run extended diagnostics on an E1 module, E1 traffic diagnostics are not performed (PD2-192644010).

Limited Commands Mode

When in limited commands mode, the slot status LED remains orange, though the link is taken down (PD2-99107226).

VDSL Modules in a Half-Duplex Link

A VDSL CPE operating in a half-duplex link can lock up when used with a hub and running wire-rate randomized traffic. This is a hardware limitation. A restart of the VDSL port will recover, but if the traffic continues at wire-rate and is randomized, then the problem will reoccur (PD2-71538118).

Summit

Summit48i Fiber Link Does Not Recover After Link Goes Down

When you configure either port 49 or port 50 to auto off speed 1000 duplex full, after you disconnect the link and plug it back in, the link on a Summit48i stays in the ready state and will not come back up (PD2-240319448).

Spurious Summit48si Power Supply Messages

When a Summit48si powers up, some power supplies might generate error messages similar to the following:

```
<INFO:SYST> PSU-A output failure recovered.
<INFO:SYST> PSU-A powered on.
<INFO:SYST> PSU-A powered off.
```

You can safely ignore these messages (PD2-208576301).

Using Vista to Add and Delete Ports

If you use Vista to add a port to a VLAN and delete that port, the port is added to the VLAN any time you add any port using Vista. To workaround this, use the CLI to add and delete ports (PD2-212786084).

Output of the show log Command

The most common reason for transceiver diagnostics failure is heat. Thus the `show log` output displays the TRXDIAG tag in the temperature log message (PD2-147462529).

The unconfigure switch all Command Clears the Default VLAN from s0

After you reset the switch to the factory defaults using the `unconfigure switch all` command, s0 does not contain the default VLAN. To add the default VLAN to s0, delete then add all ports in the default VLAN (PD2-143709201).

Health Check Error Messages

Error messages from the system health check display the incorrect location (PD2-110132842).

SNMP Results for Power Sources

The inputPower MIB is unable to differentiate between 110 V AC and 220 V AC input on the Summit series switches when accessing this MIB attribute through SNMP (10870).

Command Line Interface (CLI)

Console Does not Wait for User Input

When performing an action that requires you to confirm the action by entering `Y/N`, the console is not waiting for your reply. For example, if you issue the `unconfigure switch` command, the console should ask you to enter `Y/N` to confirm that you want to return the console to the default settings. The console skips this and does not allow you to unconfigure the switch.

Workarounds.

- Connect to the switch through the management port and issue the commands requiring user input.
- If you are using PuTTY 0.54 to connect to the switch through the console, change the terminal setting to use Ctrl+M instead of CR+LF (Telnet new line).
- Use Tera Term to connect to the switch through the console.

(PD2-247002201)

The show ports mgmt info Output Missing Flags

The output of the `show ports mgmt info` command does not display the flags (PD2-156475701).

Press [Return] Key Twice With enable temperature-log Command

You must press the [Return] key twice when entering the `enable temperature-log` command. If you only press the [Return] key once, the system does not display the asterisk indicating a configuration change. The log is correctly enabled by pressing the [Return] key once (PD2-152215201).

User Sessions Cannot Enable CLI Paging

You cannot enable CLI paging when logged in to a user account. It is enabled by default (PD2-145565305).

Switching and VLANs

The show iproute Output

The output of the `show iproute` command now displays only the first eight characters of the VLAN name (PD2-128392829).

MAC-Based VLAN Configuration Not Saved

If you configure and enable a MAC-based VLAN, save the configuration, and reboot the switch, the configuration is lost (PD2-224261163).

Load Share Group Might Fail Back to Group with Fewer Ports When Using Software Redundant Ports

If you have a primary load share group that fails over to the redundant load share group, and you remove and reinsert the I/O module that contains the primary load share group, traffic fails back to the primary load share group even though the primary load share group has fewer active ports. However, if another port in the primary group fails, traffic correctly fails over to the redundant load share group.

For example, ports 1:1-1:5 are the primary load share group and ports 2:10-2:15 are the redundant load share group. If you remove the cables from ports 1:1-1:3, the load share group fails over to ports 2:10-2:15. If you remove and reinsert the I/O module installed in slot 1 and do not attach the cables to ports 1:1-1:3, the load share group fails back to the primary load share group. If you then remove the cable from port 1:4, traffic fails over to the redundant load share group (PD2-223253601, PD2-225707301).

Saving ip-mtu Settings

Dynamic TLS (Martini TLS) checks the MTU received from its peer in order for TLS to come to the established state. It compares against the egress VLAN's IP-MTU. If the egress VLAN does not have an IP address defined, any non-default ip-mtu setting will not be saved through a switch reboot (PD2-64084527).

VLAN priority and STP, EDP

STP and EDP (thus ESRP and EAPS) do not transmit packets in the queue specified by the VLAN priority (1-5HOZ9).

Default Routes or Static Routes

If you define a default or static route, and then delete the VLAN on the subnet associated with the default route, the default route entry remains although it is invalid. You must manually delete the configured route.

If you define multiple default routes, the one with the lowest metric is used. If there are multiple routes with the same lowest metric, the switch picks one of the routes.

Configuring a Protocol Filter with 'ffff'

Creating a protocol filter with LLC of value 0xffff and assigning it to a VLAN will not work, and should not be attempted. Doing so will assign all traffic to the VLANs containing that filter and will prevent

VLANs with no protocol filter to function properly. If configured and saved, you must issue an `unconfigure switch all` to restore normal operation (2644, 4935).

Deleting Protocols from a VLAN

Adding a protocol to a VLAN may cause an EPC if the protocol was added to the VLAN, deleted from the VLAN, recreated by the user, and re-added to the VLAN (6128).

MAC Based VLANs and DHCP Relay

MAC based VLAN configurations should not be used in conjunction with DHCP. Currently, a host which enters a MAC-based VLAN will not be able to use DHCP to obtain an IP address.

VLAN to VLAN Access Profiles

VLAN to VLAN access profiles are no longer supported on the BlackDiamond switch in ExtremeWare 6.0 or higher (7022).

FDB

Cannot Add FDB Entry for Management VLAN

You cannot add an FDB entry for the management VLAN (PD2-156475718)

Static FDB Entries and Rate-Shaping

If you create a static FDB entry on a port configured for rate-shaping, the static entry incorrectly ages out. Static entries should not age out (PD2-97150551).

MAC Security

The source FDB address configuration will not discard ICMP packets (16340).

Load Sharing

Autonegotiation

Load sharing ports must be configured with autonegotiation set to on. Load sharing ports will not transmit traffic correctly using any other setting (PD2-64617405).

Round Robin Load Sharing

If a port in a round robin load share group is removed, the traffic that was being transmitted on that link will be distributed on only 1 of the other active load share links in the round robin group. The traffic is not distributed evenly between the remaining ports (6977).

Port Based Load Sharing on Summit7i

Port-based load sharing on the Summit7i requires ingress ports to be on the same side of the switch (ports 1 - 4, 9 - 12, 17 - 20, and 25 - 28 on the left, ports 5 - 8, 13 - 16, and 21 - 24 on the right) as the 8 ports in the load share group for all ports in the load share group to transmit/receive traffic (6975).

Alpine and Cross Module Load Sharing

The I/O module configured to contain the “master” port must be physically present in a cross-module load sharing group for the system to pass traffic (8589, PD2-119098401).

Load Sharing and Specific Ports in a Load Share Group

Due to the load sharing algorithm used for round robin load sharing, when using 3, 5, 6 or 7 ports in a load share group packet loss will be observed when sending wire-speed traffic across the load share group. This occurs because some ports will be selected to transmit more packets than other ports resulting in bandwidth over-subscription and subsequent packet loss. This only occurs with round-robin load sharing configurations (10311).

Disabling Load Sharing if the Master is Down Generates Error

If the load sharing master link goes down, and you disable load sharing, the switch generates a ptag error message (PD2-129379272).

ELSM

Spurious Error Message with ELSM

Disabling or enabling ELSM or the ELSM auto-restart port feature might generate an error message similar to the following:

```
hfoCliEvent: Command does not support Hitless Failover
```

You can safely ignore these messages (PD2-182478105).

Spanning Tree

Disabling ignore-bpdu Adds CPU MAC Entry to FDB

If you disable ignore-bpdu, an entry for the CPU MAC is added to the FDB for the VLAN (PD2-225957431).

Enabling STP on MAC-based VLANs Might Cause Connectivity Loss

On a BlackDiamond, if you enable STP on a MAC-based VLAN, you might experience a loss of connectivity (PD2-223958706).

Incorrect Log Message

If you reboot after enabling STP and VLANs, the device might log the following incorrect message:

```
<STP.OutBPDU.Drop> Port=8:2: Illegal message age (65517)
```

This is a display issue only; functionality is not affected (PD2-208909326).

Disabling STP Might Display Topology Change

When you disable STP, the output of the `show stpd` command displays a topology change. If there was not actually a topology change, you can safely ignore this indicator (PD2-165211765).

FDB Not Flushed After Link Failure with RSTP

When using RSTP, the FDB is not flushed when recovering from a link failure. This is the expected behavior (PD2-143730501).

Error Messages with Topology Changes

If you have STP domains configured on a switch and add active ports to the domain, bringing the links up and down might generate error messages similar to the following (PD2-159834201):

```
<Erro:STP.OutBPDU.Drop> Port=4:13: Illegal message age (21)
```

Large STPD Configuration Download Might Reboot Switch

If you download a configuration with more than 70 STP domains, and each domain has more than 120 VLANs, the switch might reboot. To avoid this, disable the system watchdog timer, download the configuration, and enable the timer (PD2-136044092).

A Large STP Configuration with 10 Link Transitions

If you have more than 120 802.1w STPDs with more than 2,000 total VLANs, a link failover might form a loop. The loop might last as long as 40 seconds, depending on the number of VLANs configured (PD2-135691018).

Configure Fewer than 4,000 VLANs in an STPD

If you add more than 4,000 VLANs to an STP domain, the switch might run out of memory (PD2-135842818).

Output of show stpName port detail Command in Hex Format

The output of the `show stpName port detail` command displays the `PortID` in hex format instead of decimal format. If you do not specify the `detail` parameter, the output correctly displays in decimal format (PD2-136044001).

If You Delete a Port from the STPD, You Cannot Add It Through a VLAN

If you delete a port from the STPD, then add a VLAN containing that port to the STPD, the deleted port is not added. To work around this, add the port back to the STPD (PD2-144382901).

The unconfigure stp Command Does Not Clear All Configurations

The `unconfigure stpd` command does not clear the tag, VLAN, operational mode, rapid root failover, port mode, or port link-type. To clear these configurations, use the `delete stpd` command (PD2-137310575).

Enabling ignore-bpdu or ignore-stp

If you enable ignore-bpdu or ignore-stp on a VLAN and then enable STP, the switch still participates in STP election. To work around this, reboot the switch (PD2-140533593).

Configuring a VLAN from Vista

If you create an STPD using ExtremeWare 6.1.9 (or earlier), add a VLAN, save the configuration, upgrade to ExtremeWare 6.2.2b68 (or later), and save the configuration, you receive the following error message when you try to modify the VLAN from Vista:

```
ERROR: Cannot assign bridge to stpd! HINT: If a port is part of multiple vlans, the
vlans must be in the same Spanning Tree domain.
```

To work around this problem, make configuration changes from the CLI (PD2-118450190).

STP and VLAN Tagging

VLAN tagging is not supported with 802.1d Spanning Tree (STP) BPDUs. Therefore, all BPDUs in a 802.1d STP domain are untagged. However, Extreme Multiple Instance Spanning Tree (EMISTP) and Per-VLAN Spanning Tree (PVST+) do support VLAN tagging of BPDUs.

EMISTP and Ingress Rate Shaping

If a loop exists in your network, but STP is not enabled and Ingress Rate Shaping is, the switches appear to hang and are rebooted by the watch-dog timer. A similar situation exists if a loop is covered by STP on both sides and is disabled on one side; normally the other switch immediately blocks the right port(s), but when Ingress Rate Shaping is present, both switches appear to hang and are rebooted by the watch-dog timer (1-5E9R1).

ESRP

The disable slot all Command Generates EDP Errors

If you have ESRP enabled, the `disable slot all` command generates EDP errors. You can safely ignore the error messages (PD2-166105101).

Large Configurations Might Lock Console when Enabling and Disabling s0

If you have more than 60 STP domains with more than 200 tagged VLANs between them and more than 6 ports in each, and you enable then immediately disable s0, the console might freeze for up to a minute. Larger networks cause the console to remain locked for longer periods. The switch is still operating, and the console unlocks after the processing finishes. To work around this, either wait before disabling s0, or wait until the console unlocks (PD2-159834277).

Hot-Swapping a Module with 5,000 ACLs

Hot-swapping a module on a switch that has 5,000 or more ACLs configured can cause an ESRP state change. To avoid the state change, configure the neighbor timeout value to 12 seconds (PD2-103938301).

ELRP

ELRP and Ingress Rate Shaping

Do not use ingress rate shaping on an ELRP-enabled VLAN (PD2-133066184).

VRRP

Backup Transition Creates Duplicate Packets

A VRRP transition from backup to master might cause duplicate data packets to be transmitted for a short period of time. The packets are dropped, so no action is required (PD2-129379226).

QoS

Duplicate Precedence Rules

If you create an ACL rule with the same precedence as an existing rule, an error message warns you of the duplication. However, the rule is still created. You must delete the rule with the duplicate precedence and recreate it with a unique precedence (PD2-116540055).

The qosprofile Accepts a Value Greater than 100%

The `maxbw` parameter in the `configure qosprofile` command incorrectly accepts values greater than 100%; however, the maximum bandwidth is still 100% (PD2-123662004).

Access Lists Using the IP Deny Any Rule

When using an access control list with an IP deny any rule, all ICMP traffic will be blocked within a VLAN (Layer 2). If using an access list with an IP deny any rule across VLANs (Layer 3), ICMP traffic will not be blocked.

Access Lists and IP Fragmentation

When using IP fragmentation, since the TCP header is treated as data and only the IP header information is being replicated in each packet, access-lists that apply to that flow will not apply as the TCP/USP port information is not included after the first fragment (for subsequent fragments).

QoS Configuration Bandwidth Parameters

Minimum and maximum percentage parameters for a specific port on the default VLAN will not be saved across reboots. The configuration change will be applied when configured. This issue only occurs on the BlackDiamond (15500).

Creating Access Lists from Multiple Sessions

When creating or modifying access control lists, please ensure that no other administrator sessions are attempting to create or modify the system access control lists simultaneously. This may result in data corruption (1-579HD).

Bi-Directional Rate Shaping

Locking and Unlocking Learning

If you configure a rate shaping port to lock learning and unlock learning, the loopback FDB is not flushed. This causes traffic destined for the port to be flooded. You must manually flush the FDB using the `clear fdb` command (PD2-124568416).

Loopback Port Must be on Same Module

The loopback port must be on the same module as the rate shaped ports. Though you can configure a loopback port on another module, this is still not a supported configuration (PD2-124299901).

1000Base-T Ports as Loopback Ports

If the loopback port for bi-directional rate shaping configurations is configured on 1000Base-T ports, the speed of that port cannot be changed from 1000 Mbps to 100 Mbps as the bandwidth settings will not be accurate when configured in 100 Mbps mode.

EAPS

Do Not Configure a Hello Time of 0

Though the minimum hello time is 1, the switch accepts a hello time of 0. Do not configure the hello time to 0, as this effectively disables EAPS (PD2-119139425).

EAPS Performance Statistics

Table 11 lists the EAPS performance statistics for a single EAPS domain with the default filter.

Table 11: EAPS performance statistics with the default filter

Protected VLANs	Link Down Convergence Upstream (ms)	Link Down Convergence Downstream (ms)	Link Up Convergence Upstream (ms)	Link Up Convergence Downstream (ms)
1	106	101	100	99
500	260	220	170	130
1,000	310	220	170	227
4,000	534	533	675	900

Table 12 lists the EAPS performance statistics for a single EAPS domain with no filters.

Table 12: EAPS performance statistics with no filters

Protected VLANs	Link Down Convergence Upstream (ms)	Link Down Convergence Downstream (ms)	Link Up Convergence Upstream (ms)	Link Up Convergence Downstream (ms)
1	1.9	1.8	1	1
500	54	54	70	100
1,000	106	106	170	226
4,000	415	415	675	900

Table 13 lists the EAPS performance statistics for a single EAPS domain with a single protected VLAN and varying FDB sizes.

Table 13: EAPS performance statistics with varying FDB sizes

FDB Entries	Link Down Convergence Upstream (ms)	Link Down Convergence Downstream (ms)	Link Up Convergence Upstream (ms)	Link Up Convergence Downstream (ms)
2,000	2.4	3.2	1.1	1.2
10,000	2.5	3.5	1.3	1.4
50,000	4	5	2.8	3
100,000	5	6	4	4

ESRP and EAPS Secondary Port

Configuring ESRP Host Attach on an EAPS secondary port causes a broadcast storm (1-B1O4L).

Incorrect show vlan Output

The `show vlan` output incorrectly lists the EAPS secondary port as active with an asterisk (*). The number of active ports is correctly displayed (PD2-59142420).

IP Unicast Routing

Reset the FDB Aging Timer

When you disable multinetting, you must reset the FDB aging timer to 300 seconds using the `configure fdb agingtime` command (PD2-160697401).

Multinetting and the show VLAN stats Command

The `show vlan stats <vlan_name>` command is not supported on multinetted VLANs (12196).

Multinetting and VRRP

Multinetting is not supported with VRRP (1-9YG1B).

RIP Routing

RIPv2 Authentication

The authentication feature of RIPv2 is not supported.

RIP in Conjunction with other Routing Protocols

It is recommended that RIP be enabled only on routers running with less than 10,000 routes from other routing protocols, such as BGP or OSPF.

OSPF

OSPF Originate Default Cost Can Be Set Incorrectly

When configuring OSPF Originate Default, an incorrect cost of 0 (zero) is accepted. If you configure the OSPF Originate Default cost to 0 (zero) the default route will not propagate (PD2-213413326).

LSA Batch Interval Not Supported

The LSA batch interval feature is not currently supported. Though you can configure the feature, (PD2-222030701).

Static Route with Switch's Address as Gateway Not Advertised

If you configure a static route with the switch's IP address as the gateway, that route is not advertised. To avoid this, do not use the switch's IP address as the gateway (PD2-222030705).

Error Message Not Generated

If you configure a low ase-limit with a lot of type-5 LSAs, enabling OSPF causes a database overflow state before OSPF adjacency is built. This should generate a critical error message, but does not (PD2-148164866).

Disable OSPF Before Adding or Removing External Area Filters

If you configure an OSPF area external filter on an ABR, and the filter is set to exclude routes that have already been learned, an OSPF failure occurs. A workaround is to disable OSPF before adding or removing OSPF external area filters (PD2-105170634).

IS-IS

Unicast Packets Considered Broadcast

Unicast packets are occasionally considered broadcast packets and dropped (PD2-142499344).

BGP

Large Number of Access Profiles and a Peer Reset

You can add a maximum of 10 BGP community numbers in inbound and/or outbound route updates using access-profiles and/or route-maps. If you add more communities, BGP might crash (PD2-160136950).

Default Route Might Not Be Deleted

If you have the export of static BGP routes enabled, the IP route table has a default static route and BGP is redistributing the default route using the `configure bgp add network` command, then after you delete the default route from BGP using the `configure bgp delete network` command, the default BGP route is not withdrawn from the neighbor's table (PD2-159150038).

BGP Aggregation with a Maximum Prefix of 300,000

Disabling BGP, configuring the maximum prefix to 300,000 or more, enabling BGP aggregation, configuring some aggregate routes, and enabling BGP generates error messages similar to the following (PD2-147347223):

```
<Erro:BGP.Misc.DelAggrtNetErr> Count lost sync for Net 202.7.243.0 Mask 255.255.255.0
```

IP Multicast Routing

The unconfigure igmp Command Does Not Unconfigure All Parameters

The `unconfigure igmp` command does not set the `forward-mcrouter-only` or `flood-list` parameters to the default values (PD2-141266115).

Enable or Disable IGMP Snooping on a Sub-VLAN

To disable or enable IGMP snooping on a sub-VLAN, delete the sub-VLAN from the super-VLAN, change the IGMP snooping status, and add the sub-VLAN to the super-VLAN (PD2-136478101).

Do Not Disable IGMP Snooping with Static Snooping Entries

If you disable IGMP snooping on a VLAN, the configured static IGMP snooping entries do not reply to the IGMP querier, while real hosts attached to the VLAN will (PD2-158477713).

Cisco Interoperation

For proper Cisco interoperation, use Cisco IOS version 11.3 or better, which supports PIM 2.0. Cisco customer support also recommends using PIM in favor of DVMRP whenever possible on Cisco routers (4669).

Traffic Rate Exceeding Last Hop Threshold

When the traffic rate exceeds the configured last hop threshold, the last hop does not initialize; but if the sending traffic rate is set to 50 Kbps, it switches to STP correctly (1-57NMY).

Security and Access Policies

Roaming Client MAC Might be Aged Out

If a network login client moves from one layer 2 switch to another switch on a different VLAN, the MAC address might be aged out and de-authenticated, generating an error message similar to the following (PD2-191169610):

```
ERROR: Port 1:3 not in vlan
```

The show netlogin Output Might Display Wrong Authentication

If you disable network login, the output of the `show netlogin` command incorrectly displays all existing authenticated 802.1x clients as HTTP. If you enable network login again, the display corrects. This is cosmetic, and does not affect the actual authentication (PD2-171477134).

ICMP Access Lists and ignore-overlap

The ignore-overlap feature is not supported with ICMP access lists. Use precedence to manage overlapping. If you specify `ignore-overlap` when you create an ICMP access list but do not specify a precedence number, a precedence of 0 is assigned. In addition, the ICMP access list gives the highest precedence to the rules created first, instead of giving precedence to the most specific rule (PD2-157416614).

CPU DoS Protect and ACL Precedence

If you configure the CPU DoS protect feature with a filter precedence of x, you cannot create an access list with a precedence of x, x+1, or x+2. All other values are acceptable.

If you configure an access list with a precedence of x, you cannot configure the CPU DoS protect feature with a filter precedence of x, x-1 or x-2. All other values are acceptable (PD2-129163428).

Network Login RADIUS Server Interoperability

The following RADIUS authentication servers are tested and supported with Network Login:

- Microsoft Windows 2000 Internet Authentication Service
- Funk Steel-Belted-Radius Enterprise Edition version 4.0

The following authentication methods are supported with Network Login:

- PAP (web-based only)
- EAP-MD5 (802.1x only)
- EAP-TLS (802.1x only)
- EAP-TTLS (802.1x only)
- PEAP (802.1x only)

Network Login Supplicant Software Interoperability

The following supplicant software applications are tested and supported with Network Login:

- Web-Based: Internet Explorer 6 web browser
- Web-Based: Netscape Navigator 7 web browser
- 802.1x: Microsoft Windows XP native OS client
- 802.1x: Microsoft Windows 2000 Professional native OS client (patch 313664)
- 802.1x: Funk Odyssey Client, version 2.0
- 802.1x: MeetingHouse Data AEGIS Client for Windows, version 2.0.5
- 802.1x: MeetingHouse Data AEGIS for Windows, version 1.3.6.1
- 802.1x: MeetingHouse Data AEGIS for Linux, version 1.1.2

RADIUS and the BlackDiamond

When RADIUS authentication is configured on a BlackDiamond switch, upon reboot, you will see the following message indicating that the system is initializing before authentication messages will be transmitted to the configured RADIUS server(s) (7046):

```
“Warning: Radius is going to take one minute to initialize.”
```

SLB and Flow Redirection

Enumeration Mode Redirects ICMP Packets

When you create a flow redirection rule for source address based on a subnet mask of /24, enumeration mode is selected, and all ICMP packets are redirected to the next hop. To work around this, use a subnet mask of /16 (PD2-118471863).

Cache Servers Set To “Down” Under Sustained High Traffic Loads

Under very high sustained loads flow redirection might fail and set a cache server to the “down” state and then bring it back up. This only occurs during high loads for a duration of more than 2 minutes. The server will come back up immediately; however, during that time connections that were established might be dropped due to a flushing of the associated IP forwarding database entries. A “down” state is depicted in the log with the following message:

```
09/01/2000 10:51.56 <INFO:IPRT> redirect next hop test <ip_addr> changed to down
```

Health Checking Cannot be Disabled

Flow redirection health checking of the next hop address is turned on by default and cannot be disabled.

NAT

NAT Rule Configuration Not Updated

If you change the name of a VLAN that is part of your NAT configuration, the NAT rule configuration is not updated. NAT rule matching continues to operate correctly, but if you save or upload the configuration, the rule is saved or uploaded incorrectly (PD2-82963707).

Vista

Failed Vista Login Logged Incorrectly

A failed Vista login appears in the syslog with the wrong IP address and login user name (PD3-11296008, PD2-203782108).

Failed Vista Login Logged Incorrectly

A failed Vista login appears in the syslog with the wrong IP address and login user name (PD2-203782108).

No 10 Gigabit Option for Port Speed

There is no 10 Gigabit option for the port speed on the port configuration page. To work around this, use the CLI (PD2-208090014).

Incorrect Minimum Limit on OSPF Page

The Miscellaneous Parameters on the OSPF page lists a minimum of zero for the costs and timers. The minimum limit is one (PD2-194279901).

Cannot Create User Accounts

You cannot create a user account using Vista; you can only create admin or pppuser accounts. To work around this, create the account using the CLI (PD2-197374642).

Cannot Enable STP

You cannot enable a STP domain using Vista. If you try, Vista does not generate an error message, but does not enable STP. (PD2-158471801).

Alpine 3808 Erroneously Displays Four PSUs

Vista displays PSU C and PSU D on an Alpine 3808 chassis. The Alpine 3808 supports only two PSUs, PSU A and PSU B (PD2-135911601)

Cannot Add Trap Receiver or Community String

On the SNMP configuration page, if you add a trap receiver or community string Vista indicates success, but does not make the change to the switch. To successfully add a trap receiver or community string, use the CLI (PD2-120713201).

Blackhole Flag Missing

The blackhole flag is missing from the FDB statistics screen (PD2-129387401).

Multicast Address Display

If you configure a routing protocol on multiple interfaces, the Vista statistics page displays the wrong Locally Registered Multicast Address (PD2-105094265).

Configuration Statistics PSU Display

The Vista configuration statistics switch display for the BlackDiamond 6808 shows four power supplies when only two are installed (1-D3RSP).

Vista and RADIUS

If a switch configured for RADIUS authentication loses communication with the RADIUS server, subsequent attempts to use the Vista Web application will take a very long time (measured in several minutes). When communication is lost with the RADIUS server, Vista will continue to make authentication requests for every page. Each request has a timer that will expire leading to an excessive amount of time to bring up each page (5144).

Configuration Options with Large Number of Interfaces

When selecting a configuration applet with a large number of configured interfaces, the traversal of the VLAN interfaces by Vista can cause a Watchdog reset due to the task utilization of Vista during the

interface data collection. It is recommended that Vista not be used for configurations with Watchdog enabled where the Vista Configuration applet is used with a large number of VLAN interfaces.

SNMP

The configure snmp community Command Replaced

The `configure snmp community` command has been replaced by the `configure snmp add community` command. Though you can enter the `configure snmp community` command, it has no effect (PD2-225385999).

Only Warm Start Smart Trap Sent After Power Cycle

When a switch is power cycled, only a warm start smart trap is sent. Previously, a cold start smart trap was sent (PD2-209311102).

Cannot Delete Default Community Strings

You cannot delete the default community strings (*public* and *private*) using the `configure snmpv3 delete community` command. To delete these strings, use the `configure snmp delete community` command (PD2-153687501).

Do Not Configure an SNMPv3 Community String with more than 32 Characters

You cannot configure an SNMPv3 community string with more than 32 characters. If you download a configuration containing such a string, that line in the configuration fails, returning the following error message to the console (PD2-150132207):

```
ERROR : SNMPV3 Community Creation Failed
```

The rest of the configuration loads correctly.

Modular Switch get Error

A get request from an NMS to a modular switch for the ifMau<object> on the management port returns a “no such instance” error (PD2-124250702).

Incrementing the Interface Value

With a getnext or bulkget on a non-existent ifIndex of an object ID, the agent returns next OID value instead of incrementing the ifIndex (2-GZ52P).

SNMP Access Profile

The access profile for SNMP read-only or SNMP read-write can be used for permit-mode only, deny-mode is not operational (7153).

SNMP and Auto-negotiation Settings

For 100/1000Base-TX ports, the ifMauAutoNegAdminStatus can only be disabled if the ifMauDefaultType is set to a speed of 100 Mbps. For 10/100Base-TX ports, you must first set the value of ifMauDefaultType to the correct setting before disabling the ifMauAutoNegAdminStatus (9416).

Extreme Fan Traps

The `extremeFanOK` and `extremeFanFailed` traps will contain the `extremeFanNumber` indicating which fan has failed (1-7J571).

Extreme Power Supply Traps

A new object was added “extremePowerSupplyNumber” to the power supply traps. The two RPS traps will no longer be sent out. Instead the extremePowerSupplyGood and extremePowerSupplyFail traps will contain the power supply number indicating which power supply has failed (1-7J56T).

Diagnostics and Troubleshooting

Errors Not Displayed in show diagnostics Output

If you run extended diagnostics, diagnosed errors are recorded in the log, but are not shown in the output of the `show diagnostics` command (PD2-225483201).

Entering q Does Not Quit Diagnostics Display

Entering `q` to quit the `show diagnostics sys-health-check` display does not quit the display (PD2-145117543).

Automatic Memory Scanning Can Trigger Incorrect Reboot Loop Detection

On Summit and Alpine switches, if memory scanning is automatically initiated via the `auto-recovery` parameter in the `configure sys-health-check` command and the reboot loop detection threshold is 1, the system might incorrectly detect a reboot loop and come up in minimal mode (PD2-140185601).

Packet Diagnostics Display Backplane Incorrectly

When you run packet diagnostics on the Alpine 3804, the console displays the backplane as slot 5. The display is wrong: the diagnostics are correctly running on the backplane. The extended diagnostics console display is correct (PD2-151752701).

Packet Diagnostics Display Wrong Slot Name

When you run packet diagnostics on the MSM in slot B, the console displays the slot as slot 10, instead of MSM-B. The display is wrong: the diagnostics are correctly running on the MSM in slot B. The extended diagnostics console display is correct (PD2-138607801).

Bus-Stats Error Messages

The `show config detail` command output displays the following new commands:

```
disable bus-stats
configure bus-stats window history 3
configure bus-stats window errors 3
configure bus-stats threshold slow-path x
configure bus-stats threshold fast-path y
```

The bus-stats feature helps filter erroneous log messages related to transient hardware errors. It is disabled by default and should only be enabled when troubleshooting transient hardware errors. Enabling this feature requires activation by Extreme Networks personnel.

Spurious Message When system-down is Configured

If you configure the system health check alarm level for system-down and a fault is detected, the switch is turned off but continuously logs the message "Card in slot N is off line." You can ignore this message (PD2-129386201).

The use configuration Command

When the switch is in minimum mode, the `use configuration` command has no effect on the backup MSM (PD2-129133801).

Output of the show diagnostics Command

The output of the `show diagnostics` command for the CPU system might display negative numbers, and the totals might not add up properly (PD2-128460401).

Configure Auto-Recovery to online or Alarm-Level to traps

If you configure the system health check auto-recovery to `offline`, save the configuration, and configure the alarm-level to `log`, a health check brings the module or switch offline regardless of how many errors the health check detects. To avoid this, either configure auto-recovery to `online`, or configure alarm-level to `traps` (PD2-124368101).

Configuring Diagnostics Mode Off

If you configure diagnostics mode OFF, and then execute the `unconfigure switch all` command, when the switch returns to active state the diagnostics mode is still set to OFF. The default diagnostics mode should be `fastpost`. To verify which diagnostics mode is set for the switch, use the `show switch` command (1-97NL1).

Disable Remote Syslog Before Enabling IPARP Debug-Tracing

With remote syslog enabled, if you configure the IPARP debug-trace to level 2 or higher, the switch hangs and is rebooted by the watchdog timer. To avoid this, disable the remote syslog prior to configuring the debug-trace (PD2-110983505).

Documentation

The Auto-Recovery Threshold Applies only to BlackDiamond I/O Modules

The auto-recovery threshold in the `configure sys-health-check` command applies only to BlackDiamond I/O modules.

Issues Resolved in ExtremeWare 7.2.0b37

The following issues were resolved in ExtremeWare 7.2.0b37. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.2.0b37 includes all fixes up to and including ExtremeWare 6.2.2b156 and ExtremeWare 7.1.1b16. For information on those fixes, see the release notes for those releases

Diagnostics

FDB scans performed on an MSM-3 no longer report false software based errors for some entries in the FDB (PD3-7844165).

Running the `reboot slot msm` command on a BlackDiamond 6816 switching MSM no longer causes the slave MSM to reboot instead (PD2-236446804).

The MSM-B, MSM-C, and MSM-D no longer get stuck in the "booted" state after running diagnostics on a BlackDiamond 6816 (PD2-231288735).

EAPS

Traffic rates no longer drop through a rate shaped port when a link goes down in an EAPS ring (PD3-10325999).

VLAN translation FDB entries are now properly programmed and traffic no longer gets blocked at EAPS switchover (PD3-7330341, PD2-245571913).

EDP

EDP now checks the slot state of the switches before transmitting the PDUs (PD2-248966897).

General

The port status LED on a Summit48si switch now blinks when the port is disabled (PD3-13003661).

The Summit7i switch now shows the power supply unit as being a 220 V power supply (PD3-1514818).

PIM

If the last-hop router and the rendezvous point (RP) are on the same switch, and the primary RP becomes unavailable, it does not take additional time for a new RP to be elected (PD2-218090789).

SLB

tNetTask no longer fails when Transparent mode server load balancing is enabled on the switch (PD3-5617550, PD2-225957479).

SNMP

When performing an SNMP query for `extremeStpDomainRstpEnabled` with STPD mode set to RSTP, the switch no longer returns a value of disabled. If STPD mode is not set to RSTP, the SNMP query for `extremeStpDomainRstpEnabled` returns a value of disabled (PD2-236033952).

All VLAN IP addresses are now shown in the walk results for SNMPwalk (PD3-5089821).

SSH

If you use PuTTY as the SSH client to access a switch, and you close the PuTTY window without first logging out, the session now ends gracefully (PD3-3039712, PD3-14925792).

STP

The STP module has been enhanced to correctly detect a loopback condition (PD3-1616711).

VRRP

Extreme Networks switches are no longer sending the ICMP redirect with the IP source address as the interface IP addressss instead of the virtual IP address (PD3-11519271, PD2-237441001).

Issues Resolved in ExtremeWare 7.2.0b33

The following issues were resolved in ExtremeWare 7.2.0b33. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.2.0b33 includes all fixes up to and including ExtremeWare 6.2.2b156 and ExtremeWare 7.1.1b16. For information on those fixes, see the release notes for those releases.

General

On a Summit48i after rebooting the system, removing and reinserting the cable no longer brings the link state to UP with autonegotiation off (PD3-3255811, PD2-248587047).

When enabling or disabling a flow redirect policy, client requests are now correctly redirected to the target device (PD2-225957494).

A flow-rule using the IPSA/IPSP combination no longer forwards other traffic from the same SA to the next-hop (PD2-238627628).

The IPSP entries in the access-list-fdb now update the new FDB entry in the STP environment (PD2-222652341).

BGP/TCP sessions are no longer closed when you Telnet from one switch to another switch that has an access-profile enabled, resulting in an ICMP port unreachable message (PD2-219911444).

Packets are now forwarding properly on GM16ti ports when load share is enabled between the Inferno and Triumph chip set based ports (PD2-222652369).

When initiating a Telnet session from an Extreme Networks switch to a Foundry Networks switch, the [Enter] key now works correctly during the Telnet session (PD2-224339872).

You no longer receive the tRootTask EPC when downloading a configuration to enable RMON (PD2-229063549).

When a redundant port is configured for load sharing, the port now activates when the module is removed or diagnostics are run (PD2-234700625).

RIP V1 routes are no longer advertised with the incorrect metric across a classful network boundary (PD2-236187230, PD2-236187250).

When issuing the `show configuration` command, the configuration sequence has been corrected for `isis lsp-refresh-interval` and `lsp-lifetime` (PD2-241094200).

Cutting and pasting the configuration file into a Telnet session no longer locks up the Telnet session because TCP is now releasing the open Telnet socket port (PD2-138423473).

In a DVMRP environment with continuos source traffic, the L3 cache is no longer deleted and recreated on every prune life time interval. The L3 cache is not deleted as long as it contains source traffic (PD2-228267476).

IP ARP checking is no longer bypassed or exited if a proxy ARP or SLB (proxy ARP entry added for VIP) is enabled (PD2-83537427, PD2-247131240).

The output of the `show fdb` command no longer displays a duplicate entry (PD2-127001501).

CLI

You can now ping both sides of the T1/E1 link multilink IPCP/BCP L2/L3 WAN links (PD2-241629501, PD2-243363701).

BlackDiamond

If you have an EAPS domain with one MSM64i installed in the master switch and two MSM-3s installed in the transit switch, the master switch no longer enters the unknown state when you initiate hitless failover on the transit switch (PD2-219743398).

BlackDiamond I/O module memory scanning and mapping support is listed in Table 14.

Table 14: Memory scanning and mapping support in BlackDiamond modules

Module	Memory Scanning and Mapping
F32Fi	Yes
F48Ti	Yes
F96Ti	Yes
G12SXi	Yes
G8Ti	Yes
G8Xi	Yes
G16x[3]	Yes
G24T[3]	Yes
WDMi	Yes
MSM-3	Yes
MSM64i	Yes

The `clear log diag-status` command is now supported on the MSM-3. Use the `clear log error-led` CLI command to clear the diag-status LED on the MSM (PD2-162199329).

Summit

When in limited commands mode, traffic is no longer forwarded (PD2-99220424).

Mirroring

IGMP snooping no longer causes multicast traffic to not be seen on a “mirror port.” Multicast traffic will resume for the IGMP Host time-out period (260 sec) (3534).

Multicast

When a unicast route is received on the transit router, the IPMC FDBs are no longer affected (PD3-829371).

Bridging

A broadcast MAC with a unicast IP no longer forwards packets twice, once in the software and once in the hardware, when IGMP snooping is disabled on the VLAN. This resulted in the broadcast packets being sent and appearing on the port on which they originally ingressed the switch (PD2-228267441).

BGP

BGP no longer crashes when handling update messages that have "unfeasible routes" whose lengths are longer than the total length of the update message (PD2-238232234).

Routes are now advertised/withdrawn properly when the same routes are exported on two IBGP peers and synchronization is disabled (PD2-241094136).

EAPS

During cross module trunking, once the slave port connection is established, EAPS no longer fails (PD2-238232220).

IP Routing

When you create an FDB entry, you can now associate multiple ports with each unicast MAC address (PD2-183714185).

If ingress and egress VLANs do not share a port, layer 3 traffic with a broadcast MAC and unicast IP address is no longer forwarded to the default route across a layer 3 boundary (PD2-119375325).

OSPF

Static routes in the routing table are now redistributed to OSPF after you use the `enable ospf export static` command (PD2-179450568).

System Related – All Systems

When you issue the `show inline-power info` command, the wrong message is no longer displayed when an over-power state is detected (PD2-217595401).

You can now use the existing pethMainPowerUsageOnNotification and pethMainPowerUsageOffNotification at the slot level using only one MIB object (PD2-218970601).

Budgeted power no longer registers a negative amount if there is a PoE blade and a Triumph blade inserted in an Alpine 3802 (PD2-224661101).

Security and Access Policies

When configuring netlogin for multiple supplicants, the login window no longer displays again after initial login, requiring each supplicant to login individually (PD2-232777155, PD2-232777162).

When using the `config inline-power` command, you can now change port detection to `discovery-test-only` (PD2-236776201).

DHCP address assignment now works correctly when you configure proxy ARP using the `always` option on the client VLAN (PD2-212809363, PD2-220954522).

STP

The STP loopback port flag is now enabled when you create a VLAN (PD2-139987618, PD2-236033931).

Adding a port to a VLAN before the VLAN is added to the STP no longer causes an error message (PD2-238308601).

When you create identical VLANs and STP domains on two connected switches and enable the STP domain, the STP Topology Change Flag is no longer always set to “true” and the topology change timer resets (PD2-213850237)

Once you enable STP on a protocol-based VLAN, the Time Since Last Topology Change no longer displays an incorrect number (PD2-224261105).

After an STP topology change, the “C” flag in the output of the `show stp` command is no longer permanently set (PD2-159151212).

Mirroring ports can now see STP BPDU packets (PD2-156960212).

After an STP topology change, the Number of Topology Changes counter in the output of the `show stp detail` command no longer continues to increment (PD2-156960201).

The flag in the output of the `show stpd ports` command no longer displays `TC` after an 802.1w topology change (PD2-115121007).

If you are using 802.1w and IGMP snooping, 802.1w topology changes no longer interrupt the multicast stream (PD2-118511373, PD2-234810401).

Do not re-use a VLAN tag if the tag is associated with an STP domain. If the VLAN tag is still being used by the STP domain, it cannot be deleted (PD2-137137230).

You no longer need to ensure a VLAN has active ports before adding the VLAN to an STP domain (PD2-137137236).

If you configure a high STP traffic load and lose a link while forwarding the traffic load, ports no longer become unstable (PD2-118500801).

After an MSM failover using hitless failover, the STP blocking port is no longer added to the FDB (PD2-225957401).

SNMP

When configuring a SNMPv3 community, there is now an encrypted keyword preceding the encrypted string, which prevents an incremental download failure (PD2-227273841, PD2-227273855).

An IP ARP based on DHCP reply packets now includes the port number of the super-VLAN or sub-VLAN configuration (PD2-214807748, PD2-247128546).

Switching and VLANs

Using the `show vlan stats` command on multiple VLANs no longer stops switch-bound ping and Telnet packets. The Summit48si no longer drops Layer 2 packets (PD2-225385621, PD2-225385634).

If the master link is disconnected when you enable trunking, the trunking port no longer remains in the disabled state after being added to the STPD (PD2-196140873).

MPLS

The `show mpls rsvp-te lsp detail` command now allows traffic to flow over RSVP-TE LSPs and TLS tunnels to be established once you enable MPLS (PD2-212771601).

VRRP

The following exception no longer occurs when setting up the VRRP task:

```
Exception
01/07/2004 20:47.30 <CRIT:SYST> Task tvrrpTask(863e1f30) failed
```

(PD2-231506748, PD2-244410201)

ESRP

After you enable ESRP on a VLAN with an IP address and no active ports, and disable ESRP on that VLAN, the route no longer becomes active (PD2-222505901).

Documentation

The ICMP Timestamp option is now disabled by default (PD2-192572201).

The typographical error “verion” has been corrected to read “version” in the following log message:

```
03/03/2004 16:11:02.74 <Crit:SYST> Slot 1 - Firmware mismatch! Expecting version
3.0, disabling PoE feature, use CLI to download appropriate firmware
```

PD2-219230901

The `advertised-class` parameter in the `config inline-power violation-precedence` command has been corrected to read `advertise-class` (PD2-237585005).

Issues Resolved in ExtremeWare 7.2.0b25

The following issues were resolved in ExtremeWare 7.2.0b25. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.2.0b25 includes all fixes up to and including ExtremeWare 6.2.2b156 and ExtremeWare 7.1.1b14. For information on those fixes, see the release notes for those releases.

General

The TCP ISN is no longer predictable (PD2-171207424).

Ping packets larger than 1472 bytes are no longer dropped when certain ACLs are configured (PD2-207734093).

When you upgrade from ExtremeWare 6.1.8 to ExtremeWare 7.0 (or later), VDSL throughput is no longer degraded with large packets (PD2-196156801).

BlackDiamond

You can now use the `reboot` command immediately after the `synchronize` command (PD2-171614101, PD2-194245901).

PoS is now supported with Spanning Tree (PD2-199020001).

If traffic into CMT ports on the master module is broadcast or has an unknown destination address, the traffic is now forwarded to the non-shared ports (PD2-197753757).

Alpine

You can now run extended diagnostics when a VDSL module is installed (PD2-116691166).

Summit

The hardware redundant ports on the Summit48i now fail over correctly when the remote port fails (PD2-183254413).

If the system health checker brings the system down due to a hardware failure, messages are now logged in the syslog, and an SNMP trap is sent (PD2-212139994).

Mirroring

Mirroring no longer might cause multicast processing to halt and report otpRamBusyWait failures in the log (PD2-133634301).

STP

Adding a port to an STP VLAN in some configurations no longer might cause the switch to crash (PD2-198602904).

Reconnecting a port in some configurations no longer creates a temporary loop (PD2-145783111).

The topology change fields in the output of the `show stpd` command now increment correctly (PD2-180096901).

ESRP

ESRP error messages are no longer generated after a reboot on a switch that has ESRP disabled (PD2-138801121).

EAPS

The EAPSstatechange trap is now sent correctly (PD2-198658077, PD2-180185834).

OSPF

You can now enable the OSPF originate-router-id feature when a loopback with the OSPF router ID is configured (PD2-151536301).

IP Multicast

The first query sent in response to a leave message has the MAX response field correctly set to the value in the last member query (PD2-134719211).

PIM

Two RP with the same priority and group address now hash using the BSR mask length (PD2-162574428).

SLB and Flow Redirection

If you specify a port number in the `disable slb node` command, the CLI no longer automatically chooses the `tcp-port-check` option, bypassing the `max-connection` option (PD2-222240739, PD2-160291501).

As the flow redirection next hop binding changes, all access lists now correctly point to the changed next hop (PD2-183691101).

Security

If you have two VLANs on the same port and one is a protocol VLAN while the other is not, but has network login enabled, the protocol VLAN now correctly passes traffic without requiring network login to be enabled and disabled (PD2-203782137).

If you are using port mapping with NAT, addresses are now correctly mapped within the configured subnet boundary (PD2-138423498).

Using SCP2 over an SSH connection now handles incorrect passwords and the abrupt closing of the session correctly (PD2-169463432).

An ACL that specifies ICMP packets now works in all scenarios (PD2-222652337).

When a network login DHCP address range is configured, DHCP queries received on unauthenticated network login ports are no longer answered by the switch when Web-based network login is disabled (PD2-190666971).

SNMP

When port 1 is added to a VLAN, an SNMP query of the ifStackTable now correctly shows the port in the 802.1q list (PD2-171207483).

You can no longer configure SNMP traps for `exceed-committed-rate` on non-Triumph ports (PD2-198566403).

If you insert or remove a GBIC, SNMP is now updated immediately (PD2-157174357).

Troubleshooting

Sliding windows are now enabled by default (PD2-192733101).

If the system health checker brings the system down, error messages now appear in the syslog (PD2-198679001).

If the system health checker is configured to bring the system down, links are correctly brought down (PD2-217607201).

Issues Resolved in ExtremeWare 7.2.0b18

The following issues were resolved in ExtremeWare 7.2.0b18. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.2.0b18 includes all fixes up to and including ExtremeWare 6.2.2b137 and ExtremeWare 7.1.1b11. For information on those fixes, see the release notes for those releases.

General

You can now use a port number as a display string (PD2-65114851, PD2-65114834).

ESRP

If you have a direct link between the master and slave switch, and that link fails, the master no longer transitions to slave and back to master (PD2-157406636, PD2-148539301).

You can now use ingress rate shaping on an ESRP-enabled port (PD2-107800933).

OSPF

When there are duplicate LSAs in the LSDB from different advertising switches, the route is now always installed in the kernel routing table (PD2-132370484).

SNMP

If you delete a static IPARP entry using SNMP, the line in the configuration creating that entry is now deleted (PD2-130505418).

Vista

In the Virtual LAN Configuration screen, the information for VLAN ports displays the correct tagging information (PD2-130140999).

Troubleshooting and Diagnostics

If you enter an event condition using the `show log events` command and press the [Tab] key for command completion, the console no longer displays an "Ambiguous token" message (PD2-153433301).

The FDB scan no longer generates spurious error messages due to scanning the FDB while the software and hardware tables are being synchronized (PD2-144096101).

The FDB scan no longer reports synchronization errors due to multiple simultaneous FDB writes and clears on Summit7i and Alpine switches (PD2-143166374).